Anno 1 - N. 10
10 ottobre/24 ottobre 2002

Boss: theguilty@hackerjournal.it

Publisher: ilcoccia@hackerjournal.it

Editor: grAnd@hackerjournal.it,

Graphic designer: Karin Harrop

Contributors: Bismark.it, Tuono Blu, Onda Quadra,

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco sul Naviglio
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00187 Roma - Piazza Colonna, 361- Tel. 06.695141 r.a.
20134 Milano, via Cavriana, 14
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.

Direttore responsabile:
Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. Parola di hacker. SCRIVETE!!!

redazione@hackerjournal.it

hack'er (hăk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

CHI SPUTA CONTROVENTO?

Come forse molti di voi avranno notato, da qualche numero questa pagina non ospita più la consueta rassegna di siti defacciati. Nel suo intento originale, questa panoramica avrebbe dovuto essere una provocazione volta ad aumentare la sensibilità sul tema della sicurezza dei siti Web. A giudicare dalle mail ricevute, la cosa è stata parecchio equivocata, e qualcuno ha pensato che noi in qualche modo approvassimo questa pratica.

Certo, non possiamo negare che qualche volta un sorrisetto è scappato, quando a essere attaccata è stata un'organizzazione o un'azienda dalla condotta discutibile, o quando il buco nella sicurezza era così macroscopico da spingere a chiedersi se il webmaster aveva mai sentito parlare di sicurezza. Di entrambe queste situazioni parliamo infatti nell'articolo di pagina 16 sul clamoroso defacement del sito RIAA, l'associazione dei discografici americani che per qualche ora si è trovata a distribuire gratuitamente Mp3 attraverso il proprio sito.

Proprio cercando l'immagine del defacement RIAA su www.zone-h.org ho avuto la conferma che abbiamo fatto la scelta giusta a prendere le distanze dai defacer. Tra i siti bucati che zone-h elenca, ho visto anche ilariaalpi.it, sito dedicato alla giornalista Rai uccisa in Somalia insieme al collega Miran Hrovatin mentre stava facendo un'inchiesta sul traffico internazionale di armi.

Complimenti ai membri della crew hax0r lab, autori della "prodezza tecnica": hanno scelto un obiettivo veramente appropriato. Che bisogno c'era di tirare giù quel sito? Ma soprattutto, "sapevano" di che sito si trattava? Probabilmente no, perché nulla lascia presumere che questi lameroni siano italiani, e perché secondo la Hall of Shame (la classifica della vergogna) di Zone-H hanno all'attivo quasi 3000 defacement, di cui la metà "di massa", segno che colpiscono un po' a vanvera.

Per loro quel sito non rappresenta un messaggio, una testimonianza, una denuncia, ma solo una macchina Linux mal configurata, grazie alla quale poter dimostrare al mondo di saper utilizzare dei programmini "punta e cracca".

Bravi, ci sono riusciti. Ma hanno anche dimostrato quanto siano idioti, grezzi e futili, e hanno rafforzato, in una schiera di persone poco informate, la convinzione che chi traffica con la sicurezza dei sistemi è senz'altro una persona spregevole.

Un suggerimento per gli hax0r: la prossima volta che vi viene voglia di divertirvi col computer, caricate Tomb Raider o visitate persiankitty.com: il tempo vi passerà ugualmente, e farete a tutti noi un grande favore.

grand@hackerjournal.it

PS: Nella pagina sostituita, come spesso accade, gli autori della "prodezza" si firmano e affermano che la loro crew è in cerca nuovi membri; per reclutarli, hanno lasciato un'indirizzo email (haxOrs@mail.com). Io ho già mandato loro i miei "commenti" personali; se volete fare altrettanto...

mailto:

redazione@hackerjournal.it

RICOMPILARE IL KERNEL

Abbiate pazienza e non consideratemi un "raddrizzaquadri", ma leggendo l'articolo sulla ricompilazione del kernel, mi sembrava mancasse qualcosa: lanciare lilo dopo aver copiato bzImage in /boot, cosa che ho sempre regolarmente fatto (e che fa anche Debian quando si installa un kernel fatto su misura). Per evitare di dire stupidaggini mi sono guardato l'ultimo kernel-HOWTO e, cito testualmente "you must re-run lilo [...] every time you create a new bzimage". Mi sembrava un fatto importante da menzionare.

DAVIDE

Giusta tirata di orecchi. Quando ci vuole ci vuole.

LINUX GRATIS: DOVE?

Volevo chiedere se l'unico altro modo per avere Linux (ad esempio Mandrake) oltre a scaricarlo (non ho una connessione abbastanza potente) è quello di comprare un pack per la modica cifra di 50 testoni (questa volta è il mio portafoglio a non essere abbastanza potente!)?

STEIUZ

Essendo Linux liberamente copiabile, ci sono tante soluzioni... Puoi fartelo (legalmente!) copiare da un amico. Se non hai amici "linuxari", cerca un gruppo di utenti nella tua zona. Puoi partire da <www.linux.it/LUG/> o, se sei all'università, dai un'occhiata nei laboratori e dipartimenti che hanno a che fare con l'informatica. Spesso questi gruppi fanno degli "Installation Party", dove puoi addirittura farti installare e configurare Linux sulla tua macchina da qualche esperto, gratuitamente. Molte riviste regalano distribuzioni Linux. Non saranno complete come quelle che si comprano nei negozi, ma il resto puoi anche scaricarlo un po' alla volta.

MA COME FANNO?

Non sono un hacker ma sono un curioso. Girovagando per la rete in cerca di notizie e trucchi circa la vostra arte mi sono imbattuto nel sito www.desktopmodels.it/hacking.htm Più giù nella pagina c'è una sessione che dice Qualcosa su di te... e il pulsante Ecco cosa c'è nel tuo PC! Ho cliccato e mi è apparso il contenuto del mio C:\ Come è possibile che abbiano potuto visualizzare il contenuto del mio Hard Disk quando io non ho nulla condiviso e addirittura Tiny Personal Firewall?

E' un banale trucco: loro non hanno alcuna possibilità di vedere il contenuto del tuo disco. Quello che in realtà succede è che il browser inserisce in un riquadro della pagina il contenuto del disco, ma non può assolutamente inviare queste informazioni all'esterno. Insomma, non è niente di diverso da quanto accade se sfogli il contenuto del tuo disco usando Explorer. Alcuni rivenditori di programmi che dovrebbero tutelare la privacy degli utenti su Internet usano un trucco simile per spaventare i potenziali clienti. Un esempio di questo tipo è il sito dal nome analogo, www.famous-models.com, segnalatoci da un altro lettori con simili perplessità. Facendo prendere ai visitatori un coccolone, sperano di vendere qualche copia in più del loro softwaraccio. Diverso il discorso di desktopmodels.it, che suona

Saremo di nuovo in edicola Giovedì 24 ottobre!

STAMPA LIBERA NO PUBBLICITÀ SOLO INFORMAZIONI E ARTICOLI

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

più come una burla. Tra l'altro, sul sito ci sono anche delle lezioni su alcune tecniche di hacking e un giochino simile a try2hack.

Porno-Journal?

Sono le 19,15 del 25/09 oggi ho comprato per la prima volta la Vs. rivista e voglio farvi i miei complimenti sia per il taglio degli articoli sia per la scelta coraggiosa di essere immuni dalla pubblicità (forse la peste del terzo millennio?? Chissà!!) entrambi molto graditi. Mosso da curiosità ho provato poco fa a connettermi col vostro sito ma... con molta sorpresa oltre che delusione sono stato ridirezionato a un sito erotico.

Angelo

Uaz! Sono andato su hackerjournal.it e ci ho trovato una pagina porno. Che succede, qualcuno ha defacciato anche voi?

MMarkk

Mannaggia, è vero. Per qualche ora i server Dns del nostro provider hanno fatto un po' i capricci, e svariati siti presenti sulla stessa macchina sono stati rimescolati a casaccio. A noi è toccato un sito chiaramente erotico, per di più infarcito di dialer per connessioni a pagamento. Ci è voluto un po' di tempo per coordinare le riparazioni tra Italia e Usa (dove risiedono i Dns incriminati), ma alla fine tutto è tornato a posto. Anche se il problema non dipendeva minimamente dalla redazione o dal Webmaster (il fido Bismark), non possiamo fare altro che scusarci per l'accaduto coi nostri lettori.

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: 3more
pass: 2tto

#HACKERJOURNAL, QUATTRO CHIACCHIERE TRA AMICI

Se vi state annoiando in ufficio, se in TV non c'è niente di bello, se l'altro PC di casa sta ricompilando un kernel o codificando un DivX e non sapete come far passare il tempo, aprite un client Irc, collegatevi a irc.azzurra.it e fiondatevi nel canale #hackerjournal. Lì ci troverete tanti altri lettori, qualche collaboratore e –se siete fortunati– persino la redazione (sempre che la produzione della rivista non sia in ritardo, e quindi piuttosto di rado purtroppo).
Per le istruzioni di base su come utilizzare Irc potete fare riferimento all'articolo apparso a pag. 22 del n. 8. In alternativa, se non volete (o non potete) installare un programma in più, potete accedere al canale anche dal nostro sito, seguendo il link "Chat".

SCUSI DOV'È IL BAR?

Sono appassionatissimo della vostra rivista. Volevo chiedervi quante uscite ci sono.

ALEX

Dalla redazione c'è una rampa di scale che porta dritta all'uscita principale; poi, se scendi ancora, ci dev'essere un'uscita sul retro dal seminterrato :-) Scherzi a parte: esce ogni quattordici giorni il giovedì.

A PROPOSITO DI OPEN SOURCE

Gentile redazione sono un esperto di sicurezza nonché vostro lettore e a proposito dei due articoli apparsi sul numero scorso e dai titoli: "Non è tutto nel panorama gratis quello che luccica" e "Hackers mezzo secolo di vittorie" vorrei esprimere il mio punto di vista a proposito dell'open source e dello shareware al giorno d'oggi.
I produttori di software shareware come sottolineato nell'articolo di grand sono stati in crisi profonda e per superare tale periodo hanno dovuto adottare delle misure discutibili, come quella di inserire degli spyware per poter sostenerne i costi di sviluppo. Altro problema, sul fronte opposto è il proliferare di multinazionali monopoliste che impongono prezzi esosi e sostanziali restrizioni nella circolazione di software, mp3 e tutto ciò che possa danneggiarne gli utili.
Oggi non si fa altro che parlare di open source, come libertà di espressione e di circolazione delle idee, e tale movimento è ammirevole per il contributo che ha dato e sta dando all'intera comunità informatica, ma non credo assolutamente che l'open source possa essere un'alternativa a lungo termine al modello commerciale al quale siamo abituati oggi. I monopoli rovinano il mercato e su questo siamo (spero) tutti d'accordo, ma di sicuro "regalare" il software non riuscirà a creare un nuovo modello di business. Lo shareware ha fallito, l'o-

pen source penso che a lungo termine possa svilire la figura dello sviluppatore, che mettendo a disposizione gratuitamente il proprio lavoro non riuscirà neppure a sostentarsi. Programmare diventerà il lusso di una stretta cerchia d'elite o di giovani che a tempo perso si possono cimentare nella creazione di programmi. Qualcuno potrebbe obiettare che nel panorama dell'open source esistono anche diversi tipi di licenza e non è corretto generalizzare, io credo invece che l'open source sia una iniziativa lodevole ma con grossi limiti, soltanto pensando ad alcuni dei suoi fautori come Stallman e Torvalds. Il primo, ha come fonte di sostentamento le donazioni di varie fondazioni, mentre il secondo è dipendente di un'azienda e non ha ricavato alcun profitto dal suo Linux (cosa che invece fanno altri per mezzo di svariate distribuzioni). Perché non tutelare anche economicamente la bravura dei programmatori? Il software è un prodotto che ha un costo, e il ritorno per i programmatori credo sia doveroso: nessuno mai si sognerebbe di regalare dell'hardware; io vi domando perché lo si dovrebbe fare col software?

PAOLO IORIO

Faccio solo alcune puntualizzazioni, lasciando la risposta "vera" a chiunque vorrà scriverci su questo argomento. Accenni al fatto che ci sono differenti licenze open source, ma questo non è un dettaglio trascurabile. Alcune di esse (quella di Sun o di Apple per esempio) non impediscono certo alle due aziende di fare fior di soldoni col software (anche se entrambe ricavano la maggior parte dei propri guadagni dalla vendita dell'hardware).
Torvalds non si è arricchito con Linux, ma senza dubbio lo ha fatto anche "grazie a Linux". Di Transmeta non è un semplice dipendente, e vorrei tanto avere il suo stesso stipendio. L'open source gli ha permesso di mettere in luce le sue capacità tecniche e organizzative, e Transmeta lo ha scelto come dirigente. La stessa cosa, magari su scala più piccola, avviene a tanti volontari delle comunità di sviluppo del software libero.

ANCORA SULLA SCUOLA...

ciao a tutti cara redazione di hacker journal,sono un 18enne e compro la vostra rivista fin dal primo numero.penso che sia stata un'ottima idea e ha aumentato di molto il mio interesse verso il settore.frequento un itis informatico,ma sono molto deluso dal fatto che di rete se ne parli solo in quinta e a livelli molto limitati.penso che si dovrebbero cambiare i programmi di queste scuole,veramente arretrati e costretti a cimentarsi per piu di un anno con programmi obsoleti quali il Pascal.Volevo una vostra impressione su questa mia idea e con questa vi faccio i migliori complimenti per la rivista.

MNOGA.

È un argomento di cui abbiamo già parlato sui numeri scorsi. Essendo l'informatica una disciplina relativamente giovane, molti degli insegnanti attuali non l'hanno mai studiata quando frequentavano le scuole o l'università. E troppi di essi, dopo aver ottenuto il loro "patentino", non hanno mai più approfondito seriamente i propri studi. Magari hanno fatto un corso di aggiornamento riguardante l'informatica, e che ha conferito loro dei punti nelle graduatorie, ma nessuno ha mai verificato che da quei corsi avessero imparato qualcosa. E a volte capita che proprio a questi tocchi insegnare ai propri studenti (che spesso ne sanno più di loro) materie che hanno a che fare col computer. Ah, riguardo al Pascal: è comunque utile e formativo imparare la struttura di un linguaggio, anche se poi non lo si utilizzerà in pratica. Meglio di niente, almeno.

DOWNLOAD DEGLI ARRETRATI

Non sarebbe possibile scaricare in un unico file gli arretrati, invece di dover scaricare le pagine singolarmente?

DANIELE C.

Sarebbe poco corretto per quegli utenti che hanno un modem lento e vogliono leggere solo alcune pagine: sarebbe molto oneroso per loro scaricare tutto quanto. Insomma, in questo modo chi vuole tutto non ci mette molto più tempo (qualche clic in più...), ma chi vuole leggere solo un articolo non deve sobbarcarsi un download dieci volte più grande.

NUOVE SFIDE

Sono un sistemista un po' tuttofare, mi occupo un po' di tutto: windows, linux, router, pix e tecnologie varie. Vorrei farvi un'appunto rispetto alla "sfida" proposta sul vostro sito: "Try2Hack".

Io sono arrivato al livello nove (KaSp3R76) e sono arrivato al punto in cui ho il "codice" per bucare il bot IRC, ma xkè nelle vostre spiegazioni non dite come sfruttare qst codice??? sarebbe + proficuo x chi vuole imparare....nn trovate???
Comunque volevo proporre altre 2 sfide presenti su internet e ke secondo me vale la pena proporre a tutti i lettori. Eccovi i link:
www.mod-x.co.uk
www.hackerslab.org

KASP3R76

Eh, lo spazio a disposizione era un po' esiguo, e abbiamo dovuto lavorare un po' di forbici in fase di impaginazione. In ogni caso, nella stessa pagina c'era il link a una guida molto più completa e presente su Internet.

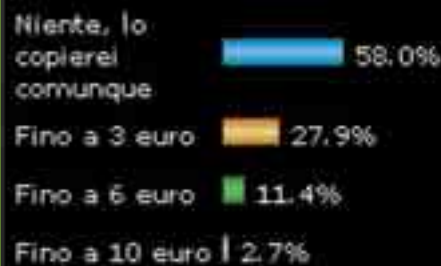
HACKER O SMANETTONI, PURCHÉ NON SI DIVENTI ALIENATI

Complimenti per la rivista, anche se secondo me era meglio chiamarla "Smanettoni Journal" che meglio si addice alla realtà underground italiana (movimento autonomo rispetto al rapporto uomo-tecnologia americano a cui spesso vi riferite).
Secondo me sarebbe meglio rimarcare, valorizzare ed enfatizzare questa differente nascita, maturazione e manifestazione della comune radice ideologica che accomuna l'Italia, l'America e qualsiasi altro paese a cui appartengono individui che amano e studiano con passione le macchine (termine sicuramente troppo freddo per descrivere i Computer!).
Anch'io appartengo al genere "Smanettoni" e ne vado fiero.Ho iniziato tutto per gioco quando ero piccolo e adesso questo interessse si è trasformato in uno studio profondo e in un lavoro a tempo pieno, regalandomi soddisfazioni e anche qualche "grattacapo"!!!
Insomma non occorre "scimmiottare" gli americani, non è importante essere etichettati come Hackers o Smanettoni, l'importante è sentirsi dentro quell'entusiasmo e quella curiosità che accomuna tutti i maniaci dei PC di tutto il mondo; qualcuno passerà alla storia, qualcun'altro no, ma non ha nessuna importanza! L'indivudualismo non deve essere confuso con l'egoismo e il fanatismo di tanti che pietosamente si definiscono Hacker!
Tutti noi abbiamo un debito di riconoscenza verso quei "pionieri del digitale" che con i loro sacrifici e la loro passione hanno dato vita a questa rivoluzione tecnologica e sociale che stiamo vivendo, a volte senza accorgercene; ora tocca a noi scegliere se ignorarla, sfruttarla oppure svilupparla e quindi sdebitarci in parte con loro. La vita è una scelta continua; un bivio dopo l'altro. Non facciamo sì che siano gli altri a scegliere per noi, prendiamoci le nostre responsabilità, cresciamo insieme e rompiamo le chiappe al mondo! Ma mi raccomando, mettete da parte l'infantilismo e non mettetevi nei guai!
Adesso mi congedo e nel salutare tutti voi voglio concludere ricordandovi che tutta la passione che abbiamo dentro non deve però degenerare in "alienazione"; il confine è molto facile da oltrepassare, e pure a me a volte è capitato. Basta crescere, imparare dai propri errori e ricordarsi che l'uomo è un "animale sociale".
L'equilibrio stà sempre nel mezzo; quando invecchieremo, i Computer non ci scalderanno come invece lo potrà fare l'amore della famiglia!

FILIPPO L.P.

Sondaggio

Quanto saresti disposto a pagare per un CD da scaricare in Mp3 dalla Rete?

Risposta	Percentuale
Niente, lo copierei comunque	58.0%
Fino a 3 euro	27.9%
Fino a 6 euro	11.4%
Fino a 10 euro	2.7%

Voti Totali: 1349

Con tre euro ci si compra a malapena il giornale, caffè e cappuccino alla mattina. Con poco di più ci comprate due copie di questo giornale. Con due, ogni quattordici giorni, ci si porta a casa Hacker Journal. Per la maggior parte dei lettori, queste cifre sono comunque un prezzo troppo alto per l'acquisto di un Compact Disc musicale. Ben il 58 percento di voi infatti pensa che, se fosse possibile acquistare un CD audio in formato Mp3, scaricandolo direttamente da Internet, lo copierebbe comunque gratuitamente, anche se costasse meno di tre miseri euro.
Dobbiamo confessare che saremmo stati molto contenti di una risposta ben diversa; molti gruppi emergenti dalla vendita di un CD ricavano molto meno di quella cifra; un atteggiamento più favorevole da parte del pubblico avrebbe potuto significare che, per molti di essi, probabilmente era più conveniente pubblicare i propri dischi sulla Rete, senza preoccuparsi troppo di produzione e distribuzione.
Con un risultato del genere, però, ho paura che ne abbiamo scoraggiati parecchi.
Ora però siamo curiosi: la risposta data era una provocazione, oppure ha qualche motivazione che non riusciamo a vedere? Fateci sapere la vostra opinione scrivendo a:
redazione@hackerjournal.it

OPEN SOURCE

Tecnici improvvisati, operatori patentati ed entità astratte

Sono un consulente informatico di 30 anni e da troppo tempo combatto una battaglia persa contro l'ignoranza che regna nel settore. Penso, in quasi 10 anni di attività, di avere studiato a sufficienza il mercato e di poter formulare una mia personale teoria.

Esistono quattro categorie fondamentali di operatori:
1) quelli che non capiscono una mazza e non sono titolati;
2) quelli che non capiscono una mazza ma sono titolati e certificati;
3) quelli che non sono né titolati né certificati ma studiano e si applicano per risolvere i problemi;
4) quelli per i quali conseguire un titolo è stato uno scherzo e che sanno tutto di tutto.

Al primo gruppo appartiene una indistinta massa di gente che riesce a campare riciclando hardware esausto e idee di altri; spesso lavorano in silenzio nei retrobottega di negozi tuttofare, che nascono e muoiono come funghi, e quando proprio vogliono strafare realizzano "software personalizzati" inutilizzabili e molto costosi, da vendere al primo sprovveduto di passaggio.

> "una indistinta massa di gente che riesce a campare riciclando hardware esausto e idee di altri"

Questi cosiddetti operatori, pur essendo i peggiori di tutto il settore sia dal punto di vista umano che professionale, svolgono una funzione essenziale di educazione del cliente il quale, dopo la prima fregatura, si rivolge a chi può dargli più garanzie.

E quando si parla di garanzie entrano in scena gli operatori del secondo gruppo: i laureati, i certificati, i patentati e tutti coloro che vedono nel titolo cartaceo una garanzia di profonda competenza e di inappuntabile professionalità.

> "non si tratta di esseri umani ma di organismi bionici che vivono in simbiosi con i calcolatori. Sono i veri protagonisti dell'innovazione tecnologica"

Questi individui spesso vivono in gruppo, in grosse organizzazioni sociali, o meglio societarie, dai nomi anglofoni e altisonanti tipo: "Corporate", "Business Unit" e via dicendo... Posseggono conoscenze limitate e molto specifiche ma sopravvivono grazie all'impiego dei temibili tecnici-commerciali: individui spietati e senza scrupoli che vendono al cliente cose di cui non ha assolutamente bisogno a un prezzo spesso spropositato.

Le persone del terzo gruppo, al quale mi pregio di appartenere, sono individui con i quali la natura è stata equilibrata; non hanno grandi doti e non eccellono in niente e proprio per questo motivo sanno di essere ignoranti! sono meticolosi e precisi ma sono anche curiosi e intraprendenti, e soprattutto sanno che per fare qualcosa, qualsiasi cosa, esiste un metodo e che come tale si può imparare e utilizzare liberamente.

Hanno competenze generiche su argomenti molto estesi ma sanno applicare un metodo rigoroso ai problemi e per questa loro caratteristica riescono a sopravvivere anche da soli.

Al quattro gruppo appartengono delle entità che vivono nella Silicon Valley, nelle leggende metropolitane e nelle voci di portineria; non si tratta di veri e propri esseri umani ma di organismi bionici che vivono in simbiosi con i calcolatori. Sono i veri e propri protagonisti dell'innovazione tecnologica.

Hanno un rapporto trascendentale con il denaro e non sopravvivono a lungo lontano dalle fonti di energia.

Detto questo, possiamo fare alcune considerazioni:
- gli operatori del primo gruppo non leggono niente;
- gli operatori del secondo gruppo leggono riviste dalle quali ricavare il maggior numero di termini anglofoni e di sigle misteriose da sputare in faccia ai concorrenti;
- gli operatori del terzo gruppo finalmente, da quest'anno, leggono la vostra rivista;
- le entità del quarto gruppo non leggono perché troppo occupate a scrivere cose difficili da capire (magari per le stesse riviste di cui sopra).

Marco S.

UN GIORNALE PER TUTTI: SIETE NEWBIE O VERI HACKERS?

NEWBIE

MID HACKING

HARD HACKING

Il mondo hack è fatto di alcune cose facili e tante cose difficili. Scrivere di hacking non è invece per nulla facile: ci sono curiosi, lettori alle prime armi (si fa per dire) e smanettoni per i quali il computer non ha segreti. Ogni articolo di Hacker Journal viene allora contrassegnato da un level: NEWBIE (per chi comincia), MIDHACKING (per chi c'è già dentro) e HARDHACKING (per chi mangia pane e worm).

LA PIÙ GRANDE FALLA NELLA SICUREZZA DI UN SISTEMA È SEMPRE L'UOMO CHE LO COMANDA

Il mistero del defacement RIAA? Elementare, caro Watson!

Il sito dei discografici antipirateria americani non è stato violato con tecniche sofisticate, ma con un pizzico di immaginazione

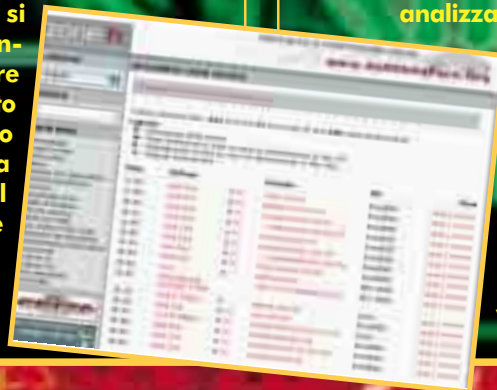
Sui numeri scorsi avevamo dato la notizia di un defacement molto particolare; la home page del sito della RIAA (l'associazione degli industriali discografici americani) era stata sostituita con un finto comunicato stampa, usando la stessa grafica del sito. Leggendo il comunicato però era facile intuire che c'era qualcosa di strano... Nel testo infatti si poteva leggere che la RIAA aveva deciso di cambiare politica nei confronti della distribuzione online di file Mp3; da quel momento i siti come Napster, Morpheus o Kazaa non sarebbero più stati perseguiti, e anzi l'associazione chiedeva scusa per le dure maniere con cui aveva fatto chiudere il servizio Listen4Ever.

A dimostrazione delle buona volontà, seguiva una piccola lista di file Mp3 che era possibile scaricare direttamente dal sito riaa.org.

Non c'è che dire, la burla è stata divertente e ben orchestrata. Ci si aspetterebbe anche che l'autore debba essere stato molto preparato dal punto di vista tecnico: bucare il sito di una delle organizzazioni che più si impegnano contro la pirateria non dovrebbe essere impresa facile. Niente di più falso: le difese adottate da questi "geni" della sicurezza erano efficaci come appiccicare sulla porta di casa un cartello con scritto "vietato prendere la chiave sotto allo zerbino", nella speranza che i ladri seguano questa indicazione. A scoprire il metodo utilizzato dai defacer sono stati Mr. Fibbles e SyS64738 di Zone-H, sito dedicato alla sicurezza informatica e che raccoglie un archivio di siti defacciati. In un divertente articolo (reperibile in inglese all'indirizzo http://www.zone-h.org/en/news/read/id=894/) hanno descritto la tecnica utilizzata.

In pratica, bastava guardare il file robots.txt del sito RIAA. Questo file viene solitamente inserito dai Webmaster in una posizione ben specifica del sito, per istruire i motori di ricerca su quali directory del sito non devono essere analizzate e indicizzate. Letto il file, lo spider del motore di ricerca ignorerà le directory elencate. Tra le directory indicate nel file robots.txt del sito RIAA ce n'era una dal nome sibillino e rivelatore: admin.

Facile intuire che doveva trattarsi della directory che conteneva i moduli per l'amministrazione del sito. A questo punto ci si aspetterebbe che il Webmaster avesse blindato quella directory, rendendola inaccessibile, e protetto i moduli con password sofisticatissime. Ancora una volta, l'ingenuità del "nostro" è disarmante: niente protezioni e nessuna password per il modulo di amministrazione. Per di più, nessun controllo sul tipo di file uploadati nella directory Pdf del sito (dove sono stati inseriti i file Mp3 da scaricare).

A più di due settimane dal defacement (che è stato operato almeno due volte), la falla nella sicurezza di riaa.org permaneva; il problema è stato risolto sette ore dopo che Zone-H aveva pubblicato la notizia. Secondo voi la Riaa si è degnata di ringraziare (anche privatamente) i nostri amici? Nemmeno per sogno, come lo stesso SyS64738 ci ha confermato. Certa gente non è proprio capace di imparare dai propri errori...

NEWS

HOT!

AVVOLTOI AL LAVORO

Non meno di 4.000 persone sono sospettate del furto di 15 milioni di dollari a un credito municipale sfruttando **una falla dei distributori automatici dopo gli attentati dell'11 settembre.** Cinquanta persone sono già state arrestate e altre 3000 sono oggetto di un'inchiesta.

ANONYMISER 2.0

Creato nel 1997, oggi Anonymiser lancia una versione tutta nuova battezzata Anonymizer Private Surfing 2. Tra le novità, **la possibilità di navigare ancora più anonimamente e più velocemente di prima.** Con questa versione la navigazione viene rallentata di appena 20 millisecondi. Un prezzo piuttosto basso, visto che i siti che visiteremo non possono identificarci. Per regalarci questa nuova versione dobbiamo sborsare 29$.

FACCIAMO ATTENZIONE!

Chi segue l'attualità della Rete, avrà notato che poco a poco il cerchio si stringe e che le libertà digitali diminuiscono inesorabilmente. E anche se ai deputati europei non piace l'idea che i log di connessione siano conservati e analizzati, il G8 spinge il più possibile per far passare il progetto di legge. Anche in Italia la questione è ampiamente discussa: i Provider preferirebbero evitare di **trasformarsi in "magazzini di dati" delle forze dell'Ordine**, che invece vorrebbero aumentare i periodi di conservazione dei log.

UN PORNOGRAFO INSEGUE AL QAEDA

John Messner è il responsabile di un sito pornografico. Passa molto tempo a navigare e non ha esitato a **utilizzare la sua tastiera come arma contro la rete terrorista Al Qaeda.** Per provocare alcuni membri della rete, li ha inondati di messaggi. Per identificarli, Messner **ha hackerato il sito Al Neda** e da allora non ha ancora smesso di inviare messaggi...

ISOLE (PRESE) NELLA RETE

L'associazione Isole nella Rete e di conseguenza il sito ecn.org **stanno rischiando grosso.** L'ex parlamentare missino Giulio Caradonna ha infatti intentato contro l'associazione e il centro sociale La Strada di Roma una **causa per diffamazione.** Oggetto del contendere è un dossier sulla storia del neofascismo in Italia, redatto dal centro sociale La Strada e pubblicato sul proprio sito, ospitato sul server di Isole nella Rete.
Nel corso dell'udienza tenutasi il 24 settembre, Caradonna ha ribadito di non avere mai guidato azioni squadriste né compiuto atti di violenza, come invece viene affermato nel dossier. Caradonna chiede una pubblica smentita e un risarcimento di 250 milioni di lire, cifra che –in caso di condanna– **metterebbe a rischio la sopravvivenza stessa dell'associazione**.
Da prima ancora della diffusione di massa di Internet, Isole nella Rete si batte per la difesa dei diritti digitali e per la libera espressione. Tutte le info sulla vicenda sono riassunte su www.ecn.org/inr/caradonna

LE VERITÀ NASCOSTE?

Questa è bella: inserendo come stringa di ricerca, tra virgolette, "go to hell" (vai all'Inferno), il motore di ricerca Google da come **primo sito rilevante niente meno che la home page di Microsoft.com.** E non è finita qui: al terzo posto si classifica la home page di **America On Line (aol.com), al quarto persino un'insospettabile Disney.com e al sesto l'emittente televisiva CNN.** Manco a dirlo, la frase incriminata non si incontra in questi siti (nemmeno nella versione della pagina memorizzata nella cache di Google). Evidentemente, qualcuno in Google ha pensato bene di divertirsi un po', oppure qualcuno di molto in gamba ha trovato il modo di alterare l'incorruttibile sistema di ranking del super motore.

ARRESTATO L'AUTORE DI T0RNKIT

La polizia inglese ha arrestato il ventunenne autore di T0rnkit, un tool utilizzato per nascondere la presenza di un intruso nei sistemi Unix. L'arresto è avvenuto in base alla legge sull'utilizzo illecito dei computer, introdotte in Gran Bretagna nel 1990; questa legge punsice i produttori e i distributori di virus, chi opera attacchi di tipo Denial of Service e chiunque penetri senza autorizzazione in un sistema informatico.
Nel caso di T0rn però non si tratta di un virus (il programma non si diffonde in modo autonomo) e nemmeno l'autore è accusato di una qualche incursione o di un'attacco DoS; **il suo reato consiste nell'aver scritto il software**.
Insomma, è un po' come se scotland Yard avesse arrestato dei ricercatori farmaceutici accusandoli del traffico internazionale di droga, o se gli autori di un libro di chimica che spiega la produzione di un esplosivo vengano incolpati di atti di terrorismo.

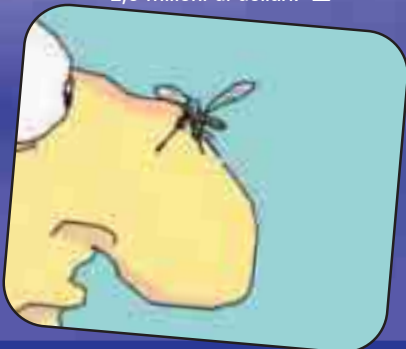
PLAYSTATION: SONY 0/PIRATI 1.

Sony è molto permalosa, si sapeva. Tuttavia, malgrado gli sforzi della società nipponica per lottare contro i “mod chip”, **non può sempre avere ragione**, e infatti ha subito un colpo nella sua lotta contro i “mod chip”, i processori che permettono alla console di leggere CD diversi da quelli per cui è stata concepita. Alla fine del mese di luglio, un giudice australiano ha decretato che questi processori un po' speciali **non violano la legislazione del paese sul copyright**. Questo riguarda le PS1 che non erano in grado di leggere i DVD. Sony aveva portato in giudizio un cittadino di Sydney per avere installato dei mod chip su numerose PS1. L'argomento del giudice contro l'azienda giapponese è che la protezione messa in atto in serie da Sony non era destinata a proteggere una tecnologia depositata, ma che si tratta di un semplice mezzo di restrizione tecnica. Tuttavia Sony ha vinto rispetto all'accusa di contraffazione, perché il cittadino di Sydney vendeva CD pirata. Il comitato per la difesa dei consumatori australiani ha dichiarato che a questo riguardo **Sony ha esagerato e che la restrizione poteva essere dannosa per i consumatori.**

WMA??? NO GRAZIE!!!

Peter Gabriel, dopo essere stato negli anni passati uno dei maggiori accusatori del P2P, si affida al formato WMA (Windows Media Audio) per la distribuzione su internet del suo ultimo lavoro. Come c'era da aspettarsi **le limitazioni ci sono e non sono poche**: 10 euro più il costo del collegamento per poter sentire i file **solo su sitemi operativi dove è possibile far girare questo formato** e la possibilità di masterizzare i brani solo su un massimo di due CD fanno ben capire che **il tutto non è conveniente**. Ancora meno conveniente se si considera che sui vari Kazaa, WinMX o Gnutella i brani sono a disposizione di tutti, in un formato ormai universale come l'mp3, supportato da tutti i sistemi operativi e da numerosissime piattaforme hardware. È aperta la scommessa sul numero di copie che Peter riuscirà a vendere…

ZANZARE SPIA NANOTECNOLOGICHE

Il futuro è della robotica e nelle nanotecnologie. La prova si trova nel lavoro di biologi e tecnici dell'università di Berkeley negli Stati Uniti, che da quattro anni cercano di mettere a punto un insetto volante micromeccanico. Malgrado quattro anni di sforzi, il successo non è ancora arrivato. L'obiettivo è **far volare un mini-robot che potrà poi, senza paura di essere scoperto, spiare tutti i nemici** che si possano immaginare. I militari sono i più interessati a questo progetto e il Pentagono è il suo finanziatore principale. Il progetto specifico dell'università di Berkeley è già costato quasi 2,5 milioni di dollari.

CERTIFICAZIONI IN CADUTA

Secondo un recente studio condotto sugli ultimi otto mesi dalla società Brainbench, **le certificazioni di sicurezza sono nettamente diminuite** dal periodo novembre 2000-luglio 2001 al periodo novembre 2001-luglio 2002. Una tendenza che tende a spiegare il calo costante del livello di sicurezza globale delle società che utilizzano le reti Internet e intranet. Il calo di certificazioni è arrivato al 22 %, un livello che comincia a diventare inquietante.

CARTA SEXY

I notabili della contea di Orange in Francia hanno recentemente deciso che **i rei di crimini di matrice sessuale saranno localizzati e i loro dati saranno pubblicati su un sito.** Un rischio per i delinquenti è che potranno avere problemi con i loro vicini. Una decisione che solleva problemi di etica nei due sensi. La motivazione delle autorità: la messa in guardia del vicinato…

UN PO' CARO MA SIMPATICO

Creative Labs ci stupisce ancora una volta con questa novità. Si tratta di un lettore di MP3 delle dimensioni di un portachiavi che non richiede cavi per essere collegato a un computer. La spiegazione di questo miracolo? **Il lettore, battezzato Creative MuVo integra una unità di memorizzazione USB removibile che si collega al PC.** Stacchiamo l'unità dal portachiavi e il gioco è fatto, possiamo trasferire i nostri file MP3. Il tutto per 150 Euro!

STEGANOGRAFIA ANTI CENSURA

Un nuovo programma promette di far vedere i sorci verdi alle autorità! Questo nuovo prodotto, basato sulle tecniche steganografiche, permette di lottare contro la censura. Il nuovo programma, **battezzato Infranet e messo a punto dal MIT**, potrà ostacolare alle misure del governo americano in materia di censura dei contenuti su Internet.

NEWS

HOT!

FACCIA TOSTA

Un Osama Bin Laden non travestito che penetra in un aeroporto avrà circa il 60% di possibilità di **essere identificato dai nuovi sistemi di riconoscimento facciale** che stanno per essere introdotti in svariati paesi. Circa una persona su cento potrebbe essere identificata per errore come Osama Bin Laden.

CARI, VECCHI TEMPI...

Ricordate che negli anni 2000 e 2001 gli attacchi di virus si succedevano uno dopo l'altro? L'inizio del 2002 si è rivelato molto più tranquillo. Per il momento il fenomeno non si spiega, anche se **sembra che i software antivirus oggi siano nettamente più potenti e performanti.** Nel corso dell'anno 2001, i virus Code Red, Nimda e Sircam avevano causato danni per miliardi di dollari. Nel 2002, a parte Klez, pochi avvenimenti importanti da segnalare.

EDUCAZIONE SESSUALE

Più del 70% dei giovani internauti cinesi **ottiene tutte le informazioni sul sesso attraverso siti Internet pornografici.** Secondo il China Daily, il fenomeno trova una spiegazione nella mancanza di educazione sessuale all'interno dell'insegnamento nelle scuole cinesi. Questi adolescenti compensano la loro mancanza di informazioni attraverso siti per adulti... Cosa non si fa per arrivare alla conoscenza!

UNA VERA SCUOLA DI HACKER

È dentro un immobile di Seattle che **un gruppo di hacker ha messo in piedi una vera scuola di hacking degna di questo nome.** Senza che nessuno sospetti niente nell'immobile, gli hacker più brillanti tracciano le falle più sottili per fare del bene e informare i siti e i provider sensibili. Battezzato GhettoHackers, questo gruppo integra tra i più brillanti pirati del momento.

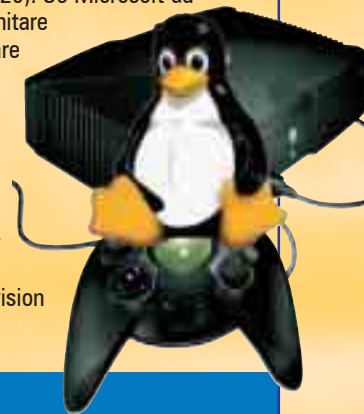
UN EX IMPIEGATO ACCUSATO

Un giovane dipendente di 21 anni è stato licenziato dopo essere stato accusato dal suo datore di lavoro di deviazione e di intercettazione delle e-mail e di reindirizzamento verso il suo sito dei visitatori del sito Web della società per cui lavorava. Il giovane, da parte sua, nega di avere violato le leggi sulla sicurezza informatica e sulla riservatezza delle informazioni personali, ma riconosce di avere intercettato alcune e-mail. Rifiuta ugualmente tutte le accuse di pirateria contro di lui da parte del datore di lavoro. Ma l'affare va ben più lontano, perché l'accusa di hacking arriva 5 mesi dopo il licenziamento del giovane presunto hacker. Ciò che ha attirato l'attenzione dell'impresa è il fatto che alcuni visitatori del suo sito Web sono stati diretti verso il sito personale dell'hacker, un sito molto virulento contro la società e con un nome eloquente.

THE IMPERIALS: ARRESTATI!

Dopo aver effettuato attacchi informatici ai danni di società del calibro TIN.it, IOL.it, Infostrada, Data Sun, Galactica, Radio 105 e diverse incursioni in alcuni server universitari, sembra che siano stati identificati e arrestati tre giovani italiani tra i 20 e i 28 anni appartenenti alla crew "The Imperials". I cracker si sarebbero traditi utilizzando numeri di carte di credito rubati per effettuare degli acquisti online. Le accuse ora sono gravi: "associazione per delinquere finalizzata alla pirateria informatica".

X-BOX: ORA È PIÙ BLINDATA.

La X-Box che verrà introdotta nei prossimi giorni avrà diverse differenze da quelle in commercio ora: si va dall'eliminazione della ventola sul chip grafico, alla sostituzione dei lettori dvd con modelli più economici. Fin qui modifiche volte ad abbassare il prezzo di produzione della console. Il vero problema sembra essere il nuovo bios che verrà implementato nelle motherboard della macchina targata Microsoft: bios completamente riscritto per l'occasione con un'unico intento, quello di rendere inutilizzabili i mod-chip che sono stati fino ad ora messi in commercio. Microsoft spera così di evitare l'utilizzo di giochi non originali o il temuto xbox-linux (che promette di far girare un sistema linux completo sulla console Microsoft, ne parliamo a pagina 26). Se Microsoft da un lato cerca di limitare l'utilizzo del software pirata non si deve dimenticare che i mod-chip servono anche per poter utilizzare software originale di importazione o per l'eliminazione della protezione Macrovision dei DVD.

IL PENTAGONO RECUPERA I SUOI PC...

Gli investigatori militari hanno messo le mani su due computer che erano scomparsi dallo Stato Maggiore dell'esercito americano in Florida. Il ladro si è ritrovato davanti quasi 50 agenti in massimo stato di allerta. I dati top secret che si trovavano sui PC riguardavano principalmente le azioni militari in Afghanistan. Il ladro era un militare e i PC sono stati ritrovati a casa sua. Per il momento non è stato ancora emessa alcuna accusa a suo carico e si ignorano i motivi del suo atto.

...MA LI PERDE IL FISCO!

Secondo un'inchiesta interna nei servizi delle imposte americani sarebbero spariti non meno di 2300 portatili! Su tali PC sarebbero presenti informazioni personali... Lo scandalo segue la sparizione di 2000 PC portatili nei servizi doganali e 400 al Ministero della Giustizia.

PALLADIUM SEMPRE PIÙ VICINO

Dopo le notizie dei giorni scorsi riguardo Intel, anche **AMD ha annunciato che sta lavorando all'introduzione del supporto del sistema di "sicurezza" Palladium**. Queste implementazioni, come noto, oltre ad impedire il funzionamento di programmi non certificati su piattaforma Windows, limiterebbe anche l'utilizzo del proprio PC in quanto un utente, molto probabilmente, non potrà più ascoltare la propria collezione di mp3 o vedere i suoi titoli in Divx. Di fatto **la libertà degli utenti sarà molto minore**. Ora che anche AMD ha deciso di collaborare a questo progetto, l'unica speranza resta quella di un terzo produttore di chip, che produca chipset Palladium-free e l'unico nome che in questi giorni circola insistentemente è quello di Transmeta (www.transmeta.com).

ADSL SI, ADSL NO

Mentre l'Autorità TLC dà il via libera a Telecom Italia per la commercializzazione di connessioni ADSL con velocità fino ai 2 Megabit, **gli utenti continuano a lamentarsi della scarsa copertura del servizio**. Moltissimi, infatti, non sono ancora stati raggiunti dal servizio e continuano a navigare con metodi più tradizionali come i 56Kb. **Il divario diventerà ancora più netto con l'ampliamento della banda** a disposizione delle persone raggiunte dal servizio, e ancora più netta sarà la differenze tra quelli che potranno usufruirne e **quelli che ormai si ritengono italiani di "serie b"**.

NON È BAGDAD CAFÈ MA KABUL CAFÈ!

Se da Riyad proviamo a collegarci per esempio al sito Internet dei Rolling Stones o al nostro sito Web personale ospitato da Geocities, rischiamo di avere una grossa delusione: questi indirizzi fanno parte dei 2.000 siti Web bloccati dal governo arabo per "preservare i valori dell'Islam". Una situazione che arriva fino all'impossibilità di accedere al sito Web della Warner Bros…
Contrariamente alla credenza popolare, l'Arabia Saudita è uno tra gli stati che applicano le più severe restrizioni di tipo religioso, principalmente sulle donne; un regime duro sostenuto da tutte le democrazie occidentali in disprezzo delle regole elementari della libertà. Solo pochi paesi limitano l'accesso a Internet dei cittadini: Vietnam, Cina ed Emirati Arabi Uniti.

"UN LINGUAGGIO CHE NON MODIFICA IL TUO MODO DI PENSARE ALLA PROGRAMMAZIONE NON MERITA DI ESSERE CONOSCIUTO"

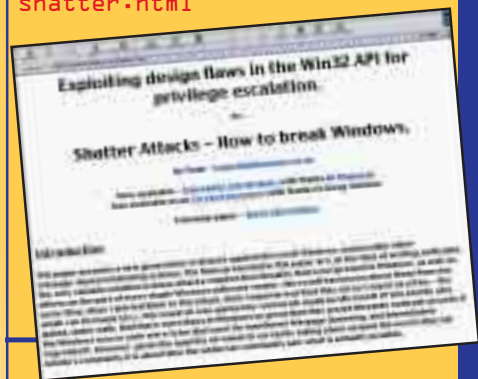
> Alex Lu, riguardo alla programmazione in Java

HOT!

FALLA CRITICA IN WINDOWS?

Un esperto britannico ha appena pubblicato un libro bianco che recensisce tutte le imperfezioni relative al sistema di gestione di Microsoft, Windows. Non è necessario dire che questo libro ha fatto digrignare i denti a Bill Gates e ad alcuni dei suoi omologhi più compiacenti. Se siete curiosi andate a consultare il rapporto su: http://security.tombom.co.uk/shatter.html

Exploiting design flaws in the Win32 API for privilege escalation.

Shatter Attacks – How to break Windows.

DECSS, ANCORA TRIBUNALI

La data del processo del giovane norvegese che ha contribuito alla creazione di DeCss (programma per decifrare il sistema crittografico dei DVD video) è stata fissata: comparirà davanti al tribunale norvegese il 9 dicembre. Un processo che comincia quasi dopo un anno dalla deposizione dell'accusa da parte della Motion Picture Association americana. Il processo era stato previsto per l'estate scorsa, ma alla fine è stato rinviato perché il giudice ha dichiarato che mancavano le conoscenze tecniche.

HARD DISK ANTI PIRATA

Si sarà trovato un modo di sconfiggere i pirati? Si, così dichiara la società giapponese Scarabs, che sostiene di aver messo a punto un metodo infallibile. L'idea sarebbe un hard disk un po' particolare dotato di due testine. Una di esse deve solo leggere i dati ed è connessa al server affinché gli internauti possano accedere ai dati; l'altra è in grado di leggere e scrivere dati, ma non è accessibile a nessuno all'infuori degli amministratori. L'idea è nata nel 1985, ma solo adesso sembra realizzabile.

HJ ha surfato per voi...

I classici della Rete

http://blackhats.it

Una comunità di ricerca sorta spontaneamente, formata da un gruppo di persone tra i quali hacker ed esperti di security. Professionisti della sicurezza informatica, molto legati al mondo underground e alla filosofia hacker. Lo fanno per proprio conto e con risorse proprie, dedicando il tempo personale a questa passione. Tra i membri della comunità, si trovano vecchie e nuove glorie del panorama dei "veri" hacker italiani. Per fare giusto un paio di nomi: Raoul Chiesa (Nobody) e Alessio Orlandi (Naif).

www.privacy.it

Uno di quei casi in cui il nome di dominio dice tutto: ci si può trovare qualsiasi cosa riguardi la riservatezza e il trattamento dei dati personali, con un occhio di riguardo per gli argomenti relativi ai computer e Internet. Dalle normative esistenti in materia, a una serie di Faq comprensibili anche a chi mastica poco il legalese. Se volete informazioni di base su quali sono i vostri diritti in materia di privacy, è uno dei primi siti da visitare.

15 minuti di celebrità! Questi sono i vostri

www.bladexperience.com

Salve, sono un vostro lettore. Prima di tutto volevo fare i complimenti alla rivista. Volevo anche segnalarvi il mio sito, a mio avviso molto interessante ;)

Mr Blade

http://www.marcodp86.cjb.net

Gentile redazione di Hacker Journal,
Vorrei segnalarvi il mio sito.
La vostra rivista è eccezionale!!! Continuate così!!!!

marcodp86

siti; sceglietе voi se tirarvela o vergognarvi

www._underground_.6go.net

(dopo aver mandato una mail con richiesta di pubblicazione del sito, ma senza indicare l'indirizzo...)

:-))) Lol diciamo che è stato un errore di battitura... Stavo scaricando a manetta e ho inviato con troppa fretta!!!
Ripeterò il mia culpa 2 volte.

Matrox

www.ipv6labs.cjb.net

Tutto ciò che riguarda il mondo dell'ipv6, sia dal lato client sia per quello che riguarda il lato server

BlAcKm[S], broly_ssj, `LYoN`,]{i||3r^1, Attila`, ^blood^, Mc\\, ChIcCa`, B|4cKSt34, Er4s3r^, sci3nc3, aNdReW, AnDrY0j`, kicco.

http://it.geocities.com/nemesishack2002

Vi vorrei segnalare il mio sito. Potete trovare: programmi, guide, e-zine, virus, immagini che fanno ridere e molto altro. Continuate così!!!

Nemesis

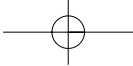
I classici della Rete

www.manuali.net

Volete sapere come si installa Linux, o come cucinare un piatto flambé? Su Manuali.net trovate corsi, lezioni, tutorial e interi manuali dedicati a questi e altri argomenti. Nato inizialmente come raccolta di manuali per l'utilizzo dei programmi, scritti direttamente dagli utenti, il sito si è espanso per abbracciare nuovi argomenti e offre anche corsi a pagamento, dal prezzo generalmente molto modico. C'è sempre da imparare...

www.telephonetribute.com

Una sorta di enciclopedia della storia del telefono, scritta da chi l'ha vissuta con entusiasmo. Dai dettagli tecnici agli aneddoti che hanno colorato la storia di alcune grandi aziende del settore (c'è anche un sito gemello che commemora il sistema Bell, su www.bellsystemmemorial.com). Nella sezione /tribute/phonephreaking.html c'è una delle più estese documentazioni sul phone phreaking e sui più famosi pirati della cornetta del telefono.

14_16_hj10_haven 2-10-2002 10:43 Pagina *14

L'ISOLA CHE NON C'É

Una piattaforma in alto mare diventa una server farm senza legge né polizia.

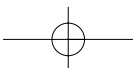
LUCI E OMBRE DEL PRINCIPATO INDIPENDENTE DI SEALAND: IL PRIMO VERO "COVO DATI"

Seconda guerra mondiale: la Gran Bretagna crea un'isola artificiale di cemento e acciaio nella parte meridionale del Mare del Nord, a circa sette miglia nautiche dalla costa inglese (latitudine 51.53 Nord, longitudine 01,28 Est per la precisione) che viene dotata di radar e armamenti pesanti e occupata da un paio di centinaia di militari. Scopo di questa operazione è difendere Londra, baluardo degli Alleati, da ogni attacco della Luftwaffe nazista. Tuttavia, con il tanto atteso cessare delle ostilità, i soldati possono tornare a casa e l'isolotto viene abbandonato e dimenticato da tutti.

>> Dimenticato da tutti?

A dire il vero non proprio tutti... Il 2 settembre 1967 Paddy Roy Bates, ex ufficiale britannico, occupò infatti la piattaforma e lì si insidiò con la famiglia proclamando ufficialmente la nascita del libero e indipendente Principato di Sealand. La risposta della Regina non tardò però a giungere e nel 1968 alcuni imbarcazioni della flotta reale si avvicinarono a Sealand ma il 'Principe' del vecchio Fort Roughs Tower, vedendo minacciato il proprio regno, intimò l'altolà alle imbarcazioni sparando alcuni colpi di avvertimento con gli stessi cannoni che un quarto di secolo prima avevano salvato Londra. In men che non si dica l'accaduto assunse portata nazionale e venne intentato un processo contro Mr. Bates; nel Novembre dello stesso anno tuttavia il tribunale dell'Essex decise di non procedere poichè, trovandosi la piattaforma ben al di fuore delle acque territoriali Britanniche (limitate a 3 miglia dalla costa), il caso era avvenuto al di fuori del territorio nazionale. In altre parole, la stessa legislazione internazionale riconosceva, seppur indirettamente, l'autonomia di Sealand rispetto alla madre patria. Sempre più determinato, Roy Bates annunciò il 25 Settembre 1975 la Costituzione del Principato e negli anni Sealand assunse sempre più la fisionomia di un vero e proprio stato, con tanto di inno nazionale, bandiera, francobolli, monete e persino targhe automobilistiche (non chiedetemi però dove parcheggino la macchina!! :)...

>> Generale, i nemici ci attaccano!

Nell'Agosto del 1978 alcuni Olandesi, capeggiati da un uomo d'affari tedesco, giunsero a Sealand per discutere di alcuni scambi commerciali con l'isolotto durante un periodo di assenza di Roy Bates; in realtà le intenzioni di questi uomini erano ben diverse e presero con la forza il controllo di Sealand sequestrando anche Michael, il figlio del 'Principe' di Sealand.

Un campo da calcetto e nulla di più; non c'è nemmeno lo spazio per bestemmiare, direbbe mio nonno!

Poco dopo però, aiutato da alcuni uomini, quest'ultimo riprese il controllo dell'isola trattenendo gli 'invasori' come 'prigionieri di guerra'. Fortunatamente quello che sembrava profilarsi come un originale incidente diplomatico senza precedenti si risolse per il meglio senza spargimenti di sangue: dopo aver invano richiesto l'intervento dell'Inghilterra, che in virtù di quanto detto in precedenza non aveva potere per intervenire nel territorio di Sealand, i Governi olandesi e tedeschi inviarono infatti sulla piattaforma Roughs Tower un diplomatico e in breve i negoziati portarono, in un primo tempo, alla liberazione degli olandesi e, in seguito, anche del cittadino tedesco.

Dopo questo episodio, Sealand smise di occupare (salvo alcune eccezioni) le prime pagine dei giornali, tornando in linea di massima ad essere più d'interesse per collezionisti e curiosi che per i diplomatici. Nel 1990 tuttavia il signor Bates attivò un'emittente radio pirata indipendente mentre nel 1997 infine un anonimo tedesco, spacciandosi per Ministro delle Finanze di Sealand, mise in vendita su Internet falsi passaporti dell'isola piazzandone più di 150.000 a 1000 Dollari l'uno; fino a quel momento invece i passaporti ufficialmente rilasciati erano stati circa 300 e nessuno di questi era stato mai venduto. Col nuovo millennio e il 'Principe' Roy, ultraottantenne, ormai stanco e affaticato, il principato più piccolo del mondo sembrava ormai prossimo alla sua fine ma...

È proprio lui, Paddy Roy Bates, principe dello stato più piccolo al mondo (e forse anche il più umido :)

Links

http://www.sealandgov.com/
Il sito ufficiale del principato di Sealand

http://www.wired.com/wired/archive/8.07/haven.html
Un dettagliato articolo di Wired sulla questione

http://www.principality-of-sealand.de/
Non lasciatevi ingannare; il sito è solo una truffa!

http://www.havenco.com/
Verrà da questa azienda il nuovo paradiso del Web?

>> Ma c'è sempre un ma...

A metà del 2000 un giovane informatico di nome Ryan Lackey ha lanciato una proposta per la creazione di un “covo dati”, nello stile di quelli descritti nel lontano 1989 da Bruce Sterling nel suo romanzo Isole nella Rete. Attratto infatti dalla situazione politica e giuridica unica al mondo di Seland (al riparo da intricate legge e dagli occhi indiscreti di agenzie investigative e al di sopra di ogni regolamentazione, restrizione, copyright, brevetto o tassa), Ryan si è dimostrato intenzionato ad utilizzare la piattaforma come sede per la propria azienda, conosciuta come HavenCo. A pochi hop di distanza dai maggiori backbone e grazie ad una connessione in fibra ottica, tramite microonde o via satellite, Sealand sarebbe infatti stata in grado di offrire una connessione ad Internet estremamente veloce ed sicura.

Una volta trovati i finanziatori del progetto, non è stato così difficile trasformare i sogni in realtà; i cilindri di cemento che sostengono la piattaforma sono così divenute stanze in grado di ospitare server e altro materiale atto allo scopo mentre guardie armate sorvegliano 24 ore al giorno il tutto e, per aumentare ulteriormente il livello di sicurezza, nemmeno ai clienti è permesso recarsi a Sealand. I "prodotti" offerti sono innumerevoli: dal semplice hosting di siti Web e di commercio elettronico a vari servizi di anonimato fino alla possibilità di offrire spazio alle aziende per lo storage di dati ehm... riservati. Tutti i dati e le comunicazioni vengono inoltre crittografati ed è possibile scegliere tra diversi sistemi operativi: Free/Net/OpenBSD, Debian GNU/Linux e RedHat Linux (è ovviamente incoraggiato l'utilizzo di UNIX e di software open source per la maggior affidabilità, sicurezza e semplicità di amministrazione remota). Inutile ricordare che una banda garantita tra i 256kbps e 1mbps, una sicurezza elevatissima e miglia di mare aperto a protezione dei dati hanno un costo: la cifra per un anno di hosting su un server nel Mare del Nord supera i 20.000 $! E' vietato utilizzare server di Sealand per inviare spam, scambiare materiale pedofilo o per lanciare attacchi di ogni tipo; a parte questi tre scopi però, come ha sostenuto lo stesso portavoce di Havenco, all'azienda non interessa quali dati contengano i server ne per quali scopi i clienti li utilizzino. Il principato di Sealand infatti non ha alcuna legge sulla privacy o sulla protezione del copyright

Sealand stuff

Sebbene sia alla guida dello stato più piccolo del mondo, Roy Bates ha fatto le cose proprio sul serio!

Come ogni stato che si rispetti, anche a Sealand sventola la bandiera nazionale; i colori sono il rosso degli eroi, il bianco dell'onore e il nero dei pirati.

La moneta circolante è il dollaro di Sealand, la cui parità è stata fissata con il dollaro statunitense.

E quale filatelico non desidererebbe avere un francobollo con il proprio volto da poter inserire nella collezione?

Lo ripeto: non soproprio dove diavolo parcheggino, ma hanno persino delle targe per auto! :)

>> Non è oro tutto quello che...

Rimane ovviamente ancora aperta la questione sulla sovranità di Seland; è infatti vero che l'Inghilterra ha più volte preferito ignorare l'esistenza di Seland riconoscendo indirettamente l'autonomia ma, d'alto canto, nessuno stato lo ha mai ufficialmente riconosciuto. Inoltre la stessa HavenCo Limited risulta fondata e regolarmente registrata in Gran Bretagna con tanto di codice identificativo (04056934) e, pertanto, soggetta a tutte le leggi della nazione. Infine da più parti, dopo i fatti dell'11 Settembre, si è indicata Sealand come una possibile futura "complice" di terroristi, che potrebbero utilizzare i servizi di HavenCo per comunicare riducendo così il pericolo di essere rintracciati.

Che anche il paradiso di Internet non rischi di traformarsi un po' in inferno?

lele - www.altos.tk

COME VEDERE SU PLAYSTATION DEI VIDEO REALIZZATI SU PC

QUESTA SERA, SUI VOSTRI SCHERMI...

Volete far vedere a un vostro amico il filmato delle vacanze o qualche video scaricato da Internet, ma questi non ha un PC né un lettore di Dvd/Video CD? Ecco come realizzare un CD che può essere visto con qualsiasi PlayStation.

Molta gente sta convertendo in Video CD i suoi filmati; oltre a costituire un **affidabile sistema di archiviazione** (meglio delle videocassette VHS), **un Video CD può essere letto anche su un lettore di DVD, e soprattutto visualizzato sulla televisione**, apparecchio che in questi casi si dimostra decisamente migliore di un monitor per PC, specialmente se di dimensioni ridotte. Se però non fosse disponibile un lettore di DVD/Video CD, ma ci fosse invece a disposizione una bella PlayStation vecchio stile? Niente paura: con un po' di ingegno e un pizzico di pazienza, **si può creare un Video CD riproducibile sulla cara Psx.**

>> Requisiti

Innanzitutto, vediamo quali strumenti ci servono:

buildcd.exe Programma DOS per creare una "preimmagine" di CD a partire da un file .CTI

stripiso.exe Programma DOS per convertire il file creato da BuildCD al formato ISO

hitlice.exe Programma DOS che "aggiusta" l'immagine ottenuta per renderla avviabile sulla Playstation.

Il pacchetto **Video4.zip**, che si scarica dall'indirizzo indicato nel box, oltre a contenere i programmi citati, contiene i seguenti file:

2352.DAT File contenente dati fondamentali da aggiungere all'immagine-creata da StripISO per permettere al CD di essere letto dalla PS

grabba.cti File di tipo CTI: esso descrive la struttura dei file e delle directory che costituiranno il nostro CD, e contiene varie informazioni sul modo in cui l'immagine del CD viene creata da BuildCD (il formato viene spiegato più avanti in questo documento).

config.dat
system.cnf
psx.exe
Questi sono i file di sistema del CD.

>>Struttura di un cd playstation

Un CD per PS ha una struttura molto particolare, sia per i file che contiene, sia per il modo in cui è masterizzato.

-I file

Per default, la Play all'accensione, cerca sul CD il file Psx.exe e lo esegue. Nel file system.cnf , però, è possibile specificare un nome differente per il file di avvio, oltre ad altri parametri che per il momento non ci interessano. In un CD "di base" per la PlayStation è anche presente un file config.dat.

Il file deve avere una struttura diversa a seconda che la Play giri su sistemi PAL (europei) o NTSC (americani).
Nel pacchetto Video4.zip ci sono due eseguibili, Psxntsc.exe e Psxpal.exe: occorre rinominare in Psx.exe quello desiderato. In entrambi i casi, si tratta di un semplice programma che visualizza uno sfondo (personalizzabile) su cui si vedono **quattro icone (personalizzabili): selezionando ognuna di esse, verrà visualizzato il filmato ad essa associato.**

-L'immagine ISO

Usare un programma "normale" (Come Easy CD Creator, fornito con molti masterizzatori) non è sufficiente per creare un CD per PS, perché esso deve avere un formato molto particolare. Occorre usare i programmi elencati sopra, nel paragrafo "requisiti" (o altri programmi equivalenti, reperibili in siti specializzati).
Vediamo la sintassi di questi programmi:

```
buildcd -ivideo.img grabba.cti
```

Questo comando crea una "preimmagine" video.img basandosi sui parametri del file grabba.cti. Se aprite un file di questo tipo, vedrete che inizia e termina con codici piuttosto complicati; quello che interessa a noi, però, è la parte centrale, che descrive la struttura delle directory del CD. Questa parte è delimitata dalle parole chiave "Hierarchy" e "EndHierarchy". Al suo interno, avremo vari "moduli", uno per ogni file e per ogni directory; quelli per i file sono delimitati da "File [nomefile.suf]" e "EndFile", mentre le directory da "Directory [nomedirectory]" e "EndDirectory". Ecco un esempio semplicissimo di struttura:

```
Hierarchy
  Directory PROVA
    File file.txt
       XASource PROVA\file.txt
    EndFile
  EndDirectory
  Directory TEST
    EndDirectory
EndHierarchy
```

Notate la parola chiave XASource che precede il nome del file, seguita dal nome del file completo del percorso che dovrà avere sul CD. La parola chiave serve a specificare che il file è di tipo XA, cioè ha una lunghezza multipla di 2048 byte; se non ce l'ha, il programma BuildCD darà un "warning", cioè un avvertimento. Una volta creata la "preimmagine", bisogna "aggiustarla" con i dati relativi al tipo di sistema su cui girerà il CD: europeo, americano o giapponese; a seconda dei casi, alla preimmagine andrà aggiunto un file diverso. Nel nostro caso, con questo comando

```
stripiso 2352 video.img video.iso
```

seguito da

```
COPY /B 2352.DAT+VIDEO.ISO CD.ISO
```

A questo punto, resta solo da "abilitare" l'immagine per girare sulla PS, con il programma Hitlice.exe: una volta avviatolo, bisogna specificare il nome completo del file .ISO da "sistemare". Dopodiché, l'immagine è pronta per essere scritta su CD... ma non con un programma qualunque come Easy CD Creator; ci vuole un programma particolare, come BlindWrite o simili. Nel pacchetto è anche presente un file .cue da utilizzare per scrivere il CD. A differenza di quanto spiegato in alcune guide presenti su Internet, questo file non è creato dai programmi contenuti nel pacchetto Video4.zip, quindi attenti a non cancellarlo quando decidete di cancellare le immagini create, per riguadagnare spazio sull'hard disk!

>>Come operare

Con questo sistema **è possibile vedere solo filmati di tipo STR** (anche se in teoria si potrebbe scrivere un programma per la Playstation che legga il formato AVI), per cui dovrete convertire i vostri filmati in questo formato; se si tratta di AVI, potete usare il programma MovieConverter. Una cosa molto importante è che **il formato dell'audio dell'AVI deve essere**

LINK UTILI

http://mikill.interfree.it/console/video4.zip
Il pacchetto contenente i file fondamentali per creare i CD per la Playstation;

www.greenspun.com/bboard/q-and-a-fetch msg.tcl?msg_id=000tS4
Forum su "VideoCD su Playstation"

www.overinside.com/piratinside/mastering/psxvideo.php
Guida alla creazione di VideoCD per la Play

http://members.xoom.virgilio.it/thematrixpj/psxvideo.htm
Come sopra.

www.gamefreax.de/toolz.html
Decine di programmi per "hackerare" la playstation!

Per vedere i VideoCD sulla playstation
www.overinside.com/piratinside/mastering/psxvideo.php

Per discutere su come vedere i VCD sulla play:
www.greenspun.com/bboard/q-and-a-fetch-msg.tcl?msg_id=000tS4

Emulatori per Playstation

EPSX EMULATOR :
www.epsxe.com

PCSX EMULATOR :
www.pcsx.net/index.shtml

http://exeat.com/ps2/ceddy/psx/
www.psxfanatics.com/

www.ngemu.com/forums/showthread.php?s=ae9c1cd4822584d516b5516e84296b3d&threadid=21379

http://help.psxfanatics.com/pcsxfaq.php

18_20_hj10_pratica 2-10-2002 12:55 Pagina 26

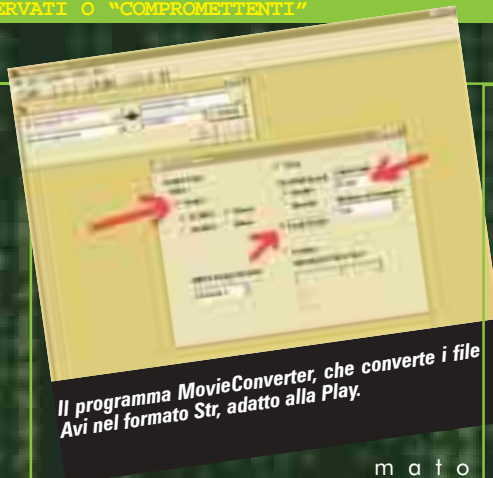
COME CANCELLARE (DAVVERO!) FILE RISERVATI O "COMPROMETTENTI"

44.100KHz, 16 bit, stereo, non compresso. Il video può invece essere anche compresso, ma la risoluzione deve essere obbligatoriamente 320x240, che è quella della Playstation.. Ricordate anche che usando MovieConverter per fare la conversione, nei parametri di conversione occorre "spuntare" la casella "Leap Sector", quella dell'audio (che deve quindi essere attivo), e impostare il frame rate (Fps) a 25. Secondo alcune guide è invece meglio impostare la frequenza a 15Fps; questo da risultati più "garantiti" ma con una minore qualità.
Una volta scompattato il file in una directory (ad esempio, C:\Psx), avremo bisogno di qualche altro programma:

TimUtil (http://mikill.interfree.it/console/timutil.zip)
Per convertire files Bmp in formato Tim e viceversa;

MovieConverter (http://mikill.interfree.it/console/movconv32.zip) Per convertire filmati Avi in Str;

STRPlay (http://mikill.interfree.it/console/strplay.zip)
Per visualizzare i filmati in formato Str.

Anche in questo caso, possiamo usare anche altri programmi che siano in grado di fare le stesse cose.
Scompattate tutti i file nella stessa directory di prima, per comodità.
A questo punto, assicuratevi di avere sottomano i quattro file Avi che vi ineteressano, e che siano tutti con audio non compresso (PCM, 44.100KHz, 16bit, stereo , ovvero qualità CD) e in formato 320x240; avviate MovieConverter, e convertiteli uno ad uno. Come già detto, usando MovieConverter per fare la conversione, nei parametri di conversione occorre "spuntare" la casella "Leap Sector", quella dell'audio (che deve quindi essere attivo), e impostare il frame rate (fps) a 25.
Terminata la conversione, rinominate i quattro file ottenuti in 1.str, 2.str, 3.str e 4.str; create una directory Video dentro la directory dove avete scompattato i file .zip, e metteteci dentro i quattro file .Str.
A questo punto, avviate in sequenza i file Grabba.bat, Grabba2.bat e Pondat.bat, oppure create un file .bat che contenga queste tre righe:

Il programma MovieConverter, che converte i file Avi nel formato Str, adatto alla Play.

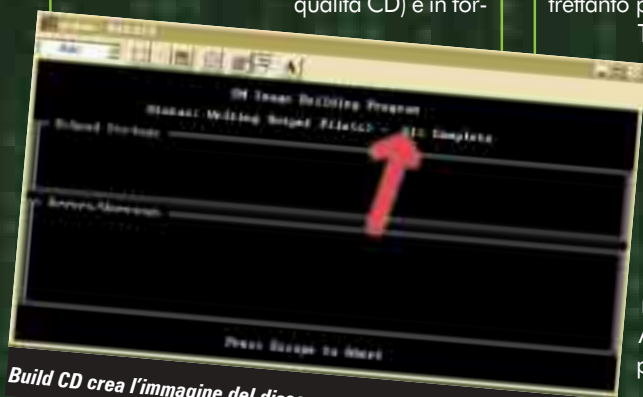
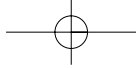
```
buildcd -ivideo.img grabba.cti
stripiso 2352 video.img video.iso
COPY /B 2352.DAT+VIDEO.ISO CD.ISO
```

L'esecuzione dei programmi potrebbe richiedere molto tempo, se i video sono molto lunghi; purtroppo, solo BuildCD mostra lo stato di avanzamento in percentuale, gli altri sembrano "bloccarsi": **in realtà, dovete soltanto aspettare**; per sapere "quanto" dovete aspettare, considerate il tempo che impiega BuildCD a terminare, e calcolate altrettanto tempo per Stripiso e altrettanto per Copy. Ci vorrà un pò...
Terminata l'esecuzione, dovrete "licenziare" la vostra immagine ISO, cioè renderla effettivamente avviabile dalla Play; attenzione, che sugli emulatori di playstation Epsx (www.epsxe.com) e Pcsx (www.pcsx.net), **l'immagine funziona anche senza usare Hitlice, ma sulla Play no**.
A questo punto, prendete il vostro programma di masterizzazione (Purché non sia Easy CD Creator 3.5c, perché non funziona) e schiaffate l'immagine su un CD. Attenzione: la play non può leggere CD riscrivibili, ma solo CD registrabili. Per non bruciare inutilmente CD, **è bene usare un emulatore di Psx, come quelli citati sopra**. Entrambi usano il sistema dei plug-in per funzionare; in altre parole, per usarli dovrete prima scaricare altri "pezzi" di programma: quello per la grafica, quello per il suono, quello per il controller, e quello per il CD-ROM, che è il più importante: gli altri possono essere qualunque, ma se usate PCSX dovrete usare un plug-in che simuli il CD tramite un file ISO. Per esempio, in questo caso dovete usare questo: http://mooby.psxfanatics.com/cdrmooby201win.zip

Build CD crea l'immagine del disco.

>>Personalizzare il programma

Con Epsx, invece, la "simulazione di CD" è di serie.
Se avete fatto tutto come si deve, avviando l'emulatore dall'immagine apparirà la schermata del programma. Potete scegliere una delle quattro icone (i tasti da usare dipendono da come avete configurato l'emulatore della play), e vedrete magicamente comparire il filmato sullo schermo della playstation... virtuale o reale che sia!
Così com'è, il programma di visualizzazione dei filmati è molto anonimo, ma non c'è problema, **la grafica è completamente personalizzabile**: lo sfondo è contenuto nel file Albums.tim della cartella Resource, e le icone sono nella cartella Icons. Convertitele in Bmp usando Timutil, modificatele come volete, riconvertitele in Tim (obbligatoriamente A 16 bit!), e ricominciate da capo la

Attenzione: in realtà, l'uso di emulatori per Playstation non è esattamente "legale", se la Playstation non l'avete. Gli emulatori, infatti, per funzionare richiedono un file contenente il BIOS della playstation, che è di proprieta' della Sony. Con PCSX o Connectix Virtual Game Station quel file non serve, viene emulato anche quello. e invece la Play l'avete, potete anche scaricare il file da Internet.

I roBOT di Irc

Nel numero precedente abbiamo visto come si crea e come si gestisce una canale, nominando molte volte dei client particolari chiamati Bot. Vedremo quindi di cosa si tratta nello specifico, dove si trovano e come si usano questi nostri potenti alleati.

Un Bot è un particolare tipo di client; non viene usato per chattare, bensì per compiere tutte quelle operazioni automatiche e ripetibili che devono essere svolte all'interno di un canale e che, effettuate a mano, **risulterebbero più lente, meno efficaci e sicuramente noiosissime**. I Bot giacciono su shell e vengono controllati in remoto dall'owner o da chi ha flag sufficienti per poterlo controlare. Un client Bot giace "inerte" compiendo i doveri per i quali è istruito senza interazione alcuna possibile con gli utenti.

Bot: forma contratta per robot; client remoto usato per compiere azioni ripetitive e per proteggere il canale.

Avendo detto che il Bot giace in remoto, vediamo di capire meglio questo concetto e di specificare cosa si intende con questo termine. **Le shell sono degli "spazi" fisici che ogni utente può acquistare su server altrui, normalmente in piattaforme Linux o FreeBSD**. Al momento della sottoscrizione del contratto, è specificata la quota di Hard Disk riservata e i processi che possono essere mandati in esecuzione. Se cercate online non vi risulterà difficile trovare una lista di server che vendono shell con caratteristiche di base simili. Ciò di cui noi abbiamo bisogno è un luogo dove sia possibile istallare uno o più Eggdrop (la versione attuale è la 1.6.12) e di tenerli in esecuzione 24h al giorno perennemente collegati alla rete.

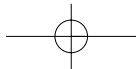
Installazione e configurazione

Dato per scontato di essercene procurata una, vediamo quali sono le azioni che si possono effettuare all'interno. Effettuato l'accesso di solito appare una schermata simile a quella della figura

Owner: è il proprietario di un Bot o una persona di sua fiducia. Ha poteri di azione illimitati sul canale e sul bot.

con un elenco dei comandi eseguibili. Date uno sguardo alla tabella per i comandi più importanti e di uso comune. Dopo aver uploadato e istallato l'eggdrop, due sono i files da compilare prima di mandare in esecuzione il proprio

Come potete vedere, dopo il collegamento SSH si apre la schermata della shell dalla quale gestirete i vostri Bots. Nel listato si possono notare alcuni comandi eseguibili.

ISTRUZIONI E TRUCCHI PER ASPIRANTI OPERATORI

Eggdrop: il file di configurazione e il file di botchk (facoltativo). All'interno dell'eggdrop che avete scaricato, troverete già dei file config precompilati; abbiate cura di leggere attentamente le istruzioni e cambiare solamente le opzioni necessarie, tenendo presente che la maggior parte di esse sono già impostate su valori mediamente validi per ogni utente. **Limitatevi pertanto a modificare solo le voci relative al nome e le altre correlate ai nomi di files e dei log di sistema**.
Il file botchk è uno script che serve per controllare periodicamente che il Bot sia attivo (up and running) e nel caso fosse trovato down per qualunque ragione, permette di riavviarlo in maniera automatica, evitando così all'owner l'obbligo di controllare spesso lo stato della Botnet. Il file giace nella directory /script e si setta col comando

```
./autobotchk -dir /home/dirdelbot
-noemail
```

In questa linea, /home/dirdelbot va sostituito con la directory dove è istallato, mentre il comando –noemail fa sì che non venga spedita un'email di avviso ogni volta che per qualche motivo viene riavviato un processo.
Ciò che è interessante e utile sapere è la struttura gerarchica di un Bot, tipica dell'ambiente Linux basato sulle flag, ma totalmente sconosciuta agli utenti windows, sistema nel quale chiunque abbia accesso al PC può fare e leggere di tutto.
Le flag sono i "permessi" attribuiti ad un utente; chiunque sia addato su un Bot ha una sua flag che risulta più o meno alta e alla quale corrispondono possibilità di azioni limitate. Il proprietario del Bot è l'owner; ha una flag +n e può compiere qualunque genere di azione. Il gradino sotto è il master, flaggato +m, e sotto ancora, come primo stadio, l'operatore, flaggato +o. Ovviamente su ogni Bot possono essere settati più owner, più master e più operatori e la scala gerarchica viene rispettata facendo sì che nessuno di grado inferiore possa compiere azioni sugli utenti di grado superiore. Esistono anche altre flag aggiuntive che attribuiscono possibilità particolari di movimento.
Tutti questi comandi vengono impartiti dalla party-line, ambiente in cui si struttura per così dire una "chat parallela" a cui hanno accesso solamente gli utenti +p e dalla quale si gestiscono i processi remoti. Per accedere alla party-line si possono utilizzare varie strategie, di certo la più comune si attua "chiamando" in DCC il Bot, azione che può essere effettuata anche da linea di comando con sintassi del tipo

```
/dcc chat nomebot
```

Strade alternative possono essere l'utilizzo del comando

```
/ctcp nomebot chat
```

o, dopo aver aperto una query,

```
chatme tuapassword
```

Flag: specifica in ambiente Linux – Unix quali azioni possono essere eseguite da ciascun utente.

Vhost: virtual host; serie di ip che si usano per suddividere le varie connessioni in modo da evitare successive disconnessioni dalla rete per "too many users (global)".

Sharare: dall'inglese to share, condividere. I Bot sharano (condividono) i database utenti in modo da lavorare sinergicamente.

LE FLAG DISPONIBILI

Flag	Descrizione
+n (owner)	E' il proprietario del bot o chiunque da lui designato
+m (master)	Utente master dei Bot
+o (op)	Utente autorizzato a farsi oppare dai Bot
+d (deop)	Chi ha questa flag non può essere oppato su un chan
+f (friend)	L'utente può floodare senza essere kikkato dal chan
+k (kick)	Kikka l'utente automaticamente
+b (bot)	E' la flag che fa riconoscere i Bot tra di loro
+p (party)	Dà accesso alla party-line
+x (xfer)	Dà accesso all'area file del Bot
+j (janitor)	Flag master dell'area file
+s (share)	Flag di Bot che permette di condividere i database
+h (hub)	Setta il Bot come principale
+a (auto)	Setta il Bot come vice-hub
+l (leaf)	Setta il Bot come secondario
+r (reject)	Rifiuta ogni connessione da quel Bot

La party-line è l'area "segreta" dei Bots. Solo gli utenti addati con flag +p vi possono accedere, ed è da qua che si programmano le istruzioni ripetitive e si impartisce ogni comando che il Bot deve eseguire.

LINK UTILI

Con qualche ricerca on-line potete trovare tutti i tutorial immaginabili sulla configurazione e soprattutto sui significati di ogni flag, insieme ai comandi utilizzabili da party-line.

www.eggheads.org
Da qui si scaricano gli eggdrop
www.egghelp.org
Sito di aiuto online per gli eggdrop
www.irchelp.org/irchelp/ircd/ircopguide.html
Guida dell'operatore di canale
www.mirchelp.org
Vari tutorials su mIRC
www.ircnet.com
Sito della rete IRCnet
www.irc.org
Altro sito su IRC
tcl.activestate.com
Sito per download di TCL per i bot
news:alt.irc.bots.eggdrop
Newsgroup dedicato ai bot di IRC

I PRINCIPALI COMANDI PARTY LINE

.adduser
Aggiunge alla lista l'utente nickname con l'hostmask (*!ident@*.dominio.it)
.binds
Mostra i bindings tcl. Cioè dei comandi scorciatoria (degli "aliases") con cui lanciare i comandi tcl
.boot
Espelle nickname dalla partyline
.chaddr
Cambia l'address di un bot per linkare il proprio alla botnet
.chattr
Cambia le flag dell'utente
.chemail
Crea o modifica l'indirizzo email nell'apposito campo informazioni utente
.chnick
Cambia il nickname dell'utente "vecchio_nick" all'interno della paryline
.chpass
Cambia la pass dell'utente
.comment
Crea o modifica i commenti per l'utente. Solo owner e master possono leggere questi commenti
.console
Permette di variare la console di sistema
.flush
Esegue la pulizia del resync-buffer del bot se le sue liste sono condivise con altri bot della botnet
.jump
Esegue il cambio di server
.link
Esegue il link alla botnet, il comando inverso è .unlink
.msg
Invia un messagio all'utente specificato
.rehash
Inizializza il bot rileggendo il file init, da utilizzare ogni volta che si esegue un cambiamento all'interno di questo file
.reload
Esegue il ricaricamento del data base utenti
.restart
Salva e ricarica la user list
.save
Negli eggdrop il salvataggio del data base utenti avviene periodicamente, ma se si vuol effettivi i cambiamenti subito, bisogna eseguire questo comando
.status Restituisce lo stato di funzionamento del bot
+host Aggiunge una nuova hostmask all'utente nickname. Il comando inverso è -host
+user Aggiunge un utente al database con l'hostmask stabilita nei parametri. Il comando inverso è -user
.+ignore Aggiunge l'utente alla ignore list. L'inverso è -ignore

Una volta dentro, la prima schermata che appare è quella di presentazione del Bot, con la versione istallata e gli utenti collegati. Per conoscere le flag dei vari utenti risulta utile il comando

```
.whois nick
```

che restituisce come output tutte le info riguardanti i vari utenti o i Bot richiesti.
È da notare come in party-line il prefisso di comando / sia sostituito dal carattere punto (.).
Essendo voi i proprietari del Bot, avrete e disposizione moltissimi comandi che dovete imparare ad utilizzare al meglio. Provate a scrivere .help e vedrete di quanti comandi siete a disposizione! Impararli tutti non è semplice e forse neppure troppo utile, ma sapere usare bene i fondamentali è di estrema importanza per non incorrere in errori che portano a perdite di tempo per la successiva riconfigurazione. Col comando .help comando si può vedere la sintassi esatta, usatelo se avete dubbi e vi eviterete grattacapi futuri.
I Bot sono altamente configurabili come è stato detto, ed in ciò ci vengono incontro degli script aggiuntivi noti come TCL. Nella tabella potrete trovare dei link da cui scaricare qualcuno di essi. Vanno inseriti all'interno del file .config e svolgono le funzioni per cui sono programmati; badate bene che ne esistono a centinaia, se non addirittura migliaia. **Sceglietele con accuratezza perché se non utilizzate correttamente possono peggiorare la vivibilità di un canale!**

>> Occhio ai conflitti

Ciò che spero sia chiaro è che il concetto su cui sono basati i Bot è quello famosissimo dell'unione che fa la forza. Tanti Bot all'interno di un canale **sarebbero quantomeno inutili se non addirittura dannosi se non fossero collegati**, linkati, gli uni agli altri. Questo link fa sì che tutti possano sharare i database ed agire sinergicamente.

Linkare: italianizzazione del verbo to link, unire. Due o più Bot linkati si passano tra di loro le impostazioni lavorando quindi all'unisono.

Vi immaginate cosa succederebbe se in un chan ci fossero alcuni Bot che impostano in automatico le modalità +stn mentre altri impostano il –t? Sarebbe una lotta continua fra chi toglie e chi mette un determinato modo di canale, cosa che porta ad un aumento di traffico di dati sul Bot, ad un rallentamento dei processi ed in ultima analisi al lag dei Bot stessi.
Vediamo quindi come evitare l'istaurarsi di questa situazione linkando i Bot tra loro.
Avendo due o più Bot dobbiamo decidere quale di questi deve essere l'hub e regolarci di conseguenza; proviamo a linkare i due Bot seguendo questo schema:

Sul nuovo Bot

.rehash
(inizializza un Bot)
.chattr nomeBot +XX
(dove XX sono le o la lettera di chi si linka, nel nostro caso A essendo unici appartenenti alla Botnet)
.+chan nomechan
(fate entrare il Bot in un chan per controllare meglio il linkaggio successivo)

Sul Bot hub

.+bot nuovoBot
.chattr nuovoBot +efoXX
(XX al solito sono le lettere dentro la botnet, nel nostro caso A)
.chaddr nuovoBot vhost:porta
(serve per la connessione telnet)
.botattr nuovoBot +gs
(flag per lo sharing dei files)
.save

Sul nuovo Bot

.+bot hub
.botattr hub +ghp
(flag per lo sharing e per indicare che quel bot è l'hub)
.chaddr hub vhost:porta
.save
.link hub

Se tutto va bene i Bot si linkano ed iniziano a sharare i database, lavorando insieme tra di loro. Oppando uno dei Bot automaticamente si oppano anche gli altri.

CAT4R4TTA
cat4r4tta@hackerjournal.it

USARE UN KEYLOGGER PER PROTEGGERE LA PROPRIA PRIVACY

COME TI SPIO

Qualcuno sbircia nel vostro computer, o lo utilizza senza autorizzazione?

Agli indirizzi www.keyghost.com e www.amecisco.com si possono trovare anche dei keylogger hardware, completamente invisibili al sistema.

"...Eppure quell'icona sono sicuro che non fosse là. Ed anche questi messaggi di posta elettronica io non ricordo di averli scaricati e letti…"
Non vi è mai capitato di trovare il vostro PC di casa o dell'ufficio con qualche differenza rispetto a quando lo avevate spento? Diciamo che forse non è proprio la norma ma può succedere. Familiari "curiosi", colleghi infastiditi dai vostri successi e dalla reputazione che vi state acquisendo col capo che cercano di sfruttare le vostre idee... sono tutte situazioni che possono compoerare una minaccia alla vostra privacy e alla sicurezza del vostro computer.

>> Il guardiano digitale

Ma come fare ad accorgersi di tali intrusioni? **Da sempre in tutti i gialli che si rispettino, la tecnica più efficace consiste nel piazzare un tranello contro il "curioso" e cercare così di coglierlo con le mani nel sacco**.
Appostamenti dietro una scrivania? Telecamere nascoste? Beh…se proprio avete tempo e soldi da perdere perché no, ma se al contrario questo non è il vostro caso, allora potete ricorrere ancora una volta alla tecnologia che ci mette a disposizione delle trappole preconfezionate e di facile uso.
Possiamo quindi installare hard disk rimovibili, programmi di crittografia e quant'altro protegga i nostri dati, ma comunque questi **sono tutti trucchi che non ci rivelano nulla sull'identità del trasgressore** che potrà continuare ad agire indisturbato.
Per raccogliere dati che ci indirizzino verso il colpevole diventa di fondamentale importanza sapere cosa esso faccia all'interno del nostro PC, a quali risorse attinga, quali sono i documenti che gli interessano e, dopo averli trovati, come li utilizza.
Come possiamo risalire a tutte queste informazioni? Beh…chiunque sa che per usare un computer si devono premere dei tasti e si cliccare con un puntatore di un mouse su qualche applicazione; ciò che noi sfrutteremo a nostro vantaggio è proprio questo "limite tecnico", facendo sì di memorizzare ogni tasto premuto ed ogni programma utilizzato dal curioso. **I KeyLoggers sono strumenti nati a questo scopo; registrano pedissequamente ogni attività**, intesa sia come applicazione eseguita che come testo introdotto, salvando tutto in un file log che risulta quindi estremamente ricco di particolari. I KeyLoggers rintracciabili su internet sono a centinaia, noi analizzeremo Windows Keylogger 5.04, ultima release di quello che forse è il più completo al momento.

>> Installazione e uso

Il programma, che si scarica dal sito **www.littlesister.de**, non necessita di istallazione; è un autoestraente che si scompatta nella directory da voi indicata. Un bel

Si inizia con le impostazioni più semplici quali l'autostart, il percorso di salvataggio del file log col suo nome ed ogni quanto tempo effettuare gli screenshots.

Nella seconda schermata si può definire l'orario di accensione e di spegnimento del programma stesso, nonché della sua autodistruzione.

Nella terza schermata si configurano le opzioni di invio tramite email del file di log.

LA SPIA

Coglietelo con le mani nel sacco, registrando tutto ciò che fa!

doppio click sull'eseguibile appena creato e il gioco inizia.
La schermata che ci si presenta altro non è che la prima delle cinque di configurazione. Il settaggio risulta assolutamente intuitivo anche se per completezza andremo ad analizzare le impostazioni più importanti.
Per far sì che si riescano a raccogliere tutte le informazioni **è necessario che il programma si avvii in maniera automatica all'accensione del computer**; in seguito dobbiamo settare il percorso dove verrà salvato il file di log. Una delle opzioni molto utili che si possono attivare in caso di bisogno consiste nella possibilità di **"scattare fotografie" di ciò che succede sullo schermo**. Queste saranno automaticamente allegate al report finale che risulterà visualizzabile come pagina web.
Nel caso in cui non vogliate, come è ovvio, che il programma registri anche le vostre attività potete impostare gli orari di accensione e di spegnimento automatico. Qualunque azione svolta sul PC fuori, per esempio, dall'orario di ufficio sarà loggata e quindi consultabile.
Avete comunque paura che il curioso scopra la vostra trappola?!?! Non temete, **attivando l'opzione di autodistruzione, il programma scomparirà magicamente alla data fissata.**

A sinistra, ecco come vi appare il file di log se ci cliccate sopra senza usare il programma di decodifica del criptaggio. Usando l'apposito programma riuscirete invece a leggere tutte le operazioni effettuate (a destra).

>> Vedere i risultati

Ah…finalmente le tanto agognate ferie…eh si, ma il vostro computer?!?! Lasciato in balia di chiunque voglia metterci le mani sopra?? Impensabile! Ecco che ancora una volta KeyLogger ci aiuta con un'opzione settabile dalla terza pagina di configurazione: l'email del log. Potete decidere di **ricevere il file ad una determinata ora oppure quando raggiunge una grandezza stabilita**; sbizzarritevi con le varie impostazioni e vedrete che anche immersi nei mari tropicali non perderete mai la possibilità di…scrutare lo scrutatore!
Ma ora che ho il file di log come lo vedo? Spero non abbiate pensato neppure per un attimo che sia sufficiente fare doppio click sul .txt…vero?!?! Come ogni programma serio che si rispetti, anche **KeyLogger implementa un sistema di cifratura dell'output** che può essere risolto solo usando un'opzione specifica nella prima pagina di configurazione del programma stesso.
Finalmente ci siamo, ecco il risultato; una serie infinita di chiarificazioni sull'uso improprio del vostro PC, corredata da immagini scattate nel desktop, salvataggi e spostamenti di documenti per arrivare infine ad ogni singolo tasto premuto. A questo punto sta solo a voi invitare il vostro amato collega a cena e farlo arrossire mettendogli in mano la stampa della sua "curiosità"…oltre che il conto, è ovvio…:D
Ma l'inganno dove sta? Effettivamente si deve ammettere che **su internet non è difficile scovare gli antiKeylogger**. Sono programmi che scannerizzano il computer e scovano i nostri "alleati". Forse a oggi una fortuna che abbiamo è che non se ne trovano molti per Windows XP e quelli che già ci sono non riescono a trovare i KeyLogger in azione. Nell'attesa di sviluppi futuri, legati in particolare al progetto Palladium di Microsoft (che dovrebbe impedire il funzionamento di simili programmi), godiamoci questa possibilità di agire indisturbati, sfruttando a costo zero questo piccolo "agente segreto" personale.

Si vedono bene anche le azioni effettuate: in questo caso il salvataggio del documento.

CAT4R4TTA,
cat4r4tta@hackerjournal.it

Attenzione a ciò che fate

L'uso che abbiamo qui descritto di un programma come Windows Keylogger è perfettamente lecito e legittimo. È però evidente che, se installato sul computer di un'altra persona, lo stesso programma può servire anche a spiare la sua privacy. In questo caso, oltre che eticamente scorretto, l'uso di un Keylogger può anche essere punito penalmente.
Se pensate che qualcun altro possa avere installato un Keylogger sul vostro computer, provate a utilizzare Anti-Keylogger, giunto alla versione 2.0. Lo trovate su
www.anti-keyloggers.com

COME INSTALLARE LINUX SU UNA CONSOLE XBOX E VIVERE FELICI

SE AL PINGUINO PIACE GIOCARE...

Prima di vedere come installare Linux su XBox, cerchiamo di capire soprattutto perchè:
- per piacere: **per immaginare la faccia di Bill Gates** appena gli arriva la notizia che il suo nipotino Basic (perchè l'avrà chiamato così...) ha rimpiazzato il contenuto della flash rom del suo XBox placcato Oro con una versione più "aggiornata", che consente l'esecuzione di codice non firmato, consente di sostituire l'hard disk con uno più capiente e che all'accensione mostra il logo "Hacked" e non più il logo Microsoft;
- per Dovere: **un computer capace di 1Gigaflop con 8(10)giga di disco e 64 mega di memoria non vanno sprecati** a giocarci a "fifa 2002";
- per Necessità: se ho voglia di **vedermi i DivX sulla Tv**? Se ho voglia di **guardare www.hackerjournal.it e non ho voglia di accendere il PC**? Se ho voglia di **ricompilare il kernel mentre guardo Xfiles**?

Una tastiera usb connessa a XBox tramite un hub.

Uno dei Player DivX disponibili .

>>Da dove comincio?

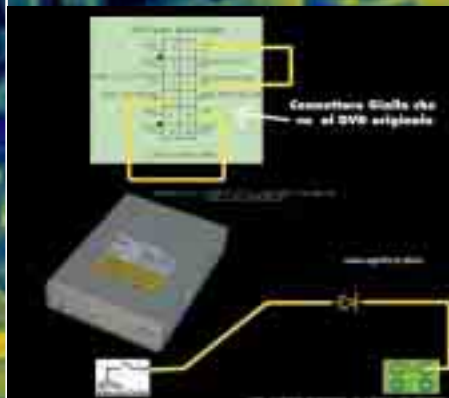
Per compinciare, abbiamo bisogno di XBox con Controller, Modchip (possibilmente con flash facilmente aggiornabile; io uso PcBioxx) e del Firmware per modchip (io utilizzo la mia versione [Kina Release] di ComplexBios 1.02)

Facciamo finta che ho modificato la mia XBox e ho sostituito la dashboard originale (quella specie di groviglio di tubi verdi in 3d) con EvolutionX.

Navigo su http://XBox-linux.sourceforge.net e decido cosa provare:

Ed's XBox Linux Live CD
(http://sourceforge.net/project/showfiles.php?group_id=54192)
Questa mini distribuzione contiene un mare di roba compreso mplayer, **un efficace lettore di video** che digerisce svariati formati e codec (divx/mp3/xvid/dvd/mpeg player). Basta masterizzare in un CD-RW l'immagine ISO scaricata, inserire il CD nella console e ripartire.

Non avendo una tastiera USB **si può accedere a LinBoX tramite ssh** all'indirizzo 192.168.0.2, altrimenti è necessario **modificare una delle porte joypad affinchè diventi una porta USB standard**, sulla quale connettere una tastiera usb (io utilizzo una tastiera per sony PS2!!). Nella distribuzione sono inclusi anche tutti i tool di sviluppo e varie network utilities.
La password per root è: XBox

XBox-linux.0.4.zip
(http://cvs.sourceforge.net/cgi-bin/viewcvs.cgi/XBox-linux/binary/iso-images)
Questa è l'ultima versione attualmente disponibile, rilasciata un paio di settimane fa da Milosh Meriac. Contiene supporto per tastiera e mouse USB, tutte le schede di rete usb attualmente supportate da Linux, supporto per hub usb, controller XBox e joypad vari.
Questa è la prima release a permettere l'esecuzione di X e di twm. In questa minidistribuzione (3 Mega) è incluso un player Mp3/divx e utility varie.

Schema di collegamento del Drive Aopen.

L'XBox di Microsoft è a tutti gli effetti un computer su cui potrebbe girare un sistema operativo serio: perché limitarsi a usarlo per giocare?

>>Passiamo all'utilizzo di LinBoX

La password per root è: rootme
L'accesso all'hard disk dell'XBox ancora non è consentito. **Il disco dell'XBox è bloccato tramite l'IDE Password Block** e il filesystem utilizzato è una variazione di Fat32. In questo momento Michael Steil e SpeedBump non hanno ancora rilasciato i drivers fatx e il modulo necessario a sbloccare l'hard disk ma dovrebbe essere imminente. Per ora, le uniche soluzioni per cominciare a produrre qualcosa prevedono di montare un disco NFS, attaccare all'XBox un disco USB, oppure sostituire il disco dell'XBox con un altro disco IDE non "FatX" e non "Password Protected". **Il tasto Eject del DVD-EOM attualmente causa il reboot della console**, ci sta lavorando TJ Fontaine. Nella mia XBox ho sostituito il drive originale con un Aopen 1648, per cui posso espellere il DVD utilizzando il tasto eject del drive. Vi ricordo che il drive originale di XBox è in grado di leggere a malappena alcuni CD-RW (non tutti) e non legge i CD-R (monta un'ottica singolo pickup) e con i CD-RW è molto (mooooolto) lento. Esistono trucchi come tentare di calibrare il laser affichè possa leggere più facilmente i CD-RW, ma **è un'operazione molto rischiosa: facilmente salta il laser del drive**. Nella foto in queste pagine potete vedere come collegare il drive.
Per collegare uno o più dispositivi USB occorre sostituire una delle porte gamepad di XBox con una porta usb standard,io ne ho utilizzata una estratta da un adattatore usb interno per pc. Ho dovuto "segare" il connettore del joypad, incollare il connettore usb e connettere i fili che da XBox portano al connettore joypad segato. I connettori joypad sono porte usb standard a cui è stato aggiunto un quinto filo per poter gestire dispositivi come pistole e penne ottiche. I colori dei cavi sono quelli definiti dallo standard USB, per cui basta connettere i cavi rosso, verde, bianco e nero con il corrispondente. Connettendo un hard disk USB, consiglio di **utilizzare o un HD alimentato esternamente o di utilizzare un hub alimentato**, per evitare di sovraccaricare il circuito USB interno a XBox.
Per installare LinBoX su hard disk (in modo da poter utilizzare dei DivX su CD-ROM) bisogna procurarsi xbeboot già configurato per partire dall'HD, oppure ricompilarlo commentando opportunamente il file XBox.h affinchè parta dall'harddisk. Per fare ciò bisogna sostituire la riga

```
#define CONFIG_FILE "\\
Device\\Cdrom0\\linuxboot.cfg"
```

con

```
#define CONFIG_FILE "\\Devi-
ce\\Harddisk0\\Partition1\\
Apps\\Linux\\linuxboot.cfg"
```

In seguito bisogna editare il file linuxboot.cfg, per es:

```
ROOT  \Device\Harddisk0\Parti-
tion1
KERNEL \apps\LinBoX\vmlinuz
INITRD \apps\LinBoX\initrd.gz
```

Tramite evolutionX e Flashfxp copiare i file initrd.gz, vmlinuz, linuxboot.cfg e il default.xbe appena compilato, editare il menu.ini di e...

Una schermata Linux su XBox

Dettaglio del collegamento porta USB su XBox.

>> ...e vai con LinBoX!

All'avvio della nostra LinBox vedremo per primo un grosso pinguino al centro dello schermo, se questa schermata è presente, significa che il loader del sistema operativo (default.xbe) funziona a dovere. Dopo pochi secondi appariranno in alto il famoso logo di Xbox-LinuX e di seguito tutte le normali informazioni di debug che si hanno allo start-up di Linux, il processore, il controller ide, il controller usb, i dischi, il Dvd-Rom, la scheda di rete vengono riconosciuti correttamente alla fine del processo di startup potremo fare il login come root o come guest/guest e cominciare a smanettare. In questo momento il driver video è utilizzato in maniera "Frame-Buffer" per cui **non si ha alcuna accelerazione hardware**. Inoltre la modalità di default del encoder interno per l'uscita TV è in modalità Overscan per cui, in particolar modo in console/TV PAL, **non potremo vedere i bordi dello schermo, cosa che rende difficoltoso operare** (non si vede il prompt) la risoluzione del problema è prossima, intanto vi consiglio di utilizzare il LinBox da telnet/ssh (ifconfig per vedere che indirizzo è stato impostato) o tramite un pc con ingresso video o con un vecchio monitor PAL per C64 ;-))). Non resta che installare LinBox e smanettarci sopra.

Vincenzo Agrillo "KinaWeb"

SI STA DIFFONDENDO SEMPRE PIÙ LA RETE SENZA FILI: MA GARANTISCE LA NECESSARIA SICUREZZA?

Sicurezza nell'etere

Con il protocollo 802.11b è possibile tagliare i cavi Ethernet e navigare ad alta velocità in rete. Ma quanto può definirsi sicuro questo sistema? Analizziamo insieme lo standard, il protocollo e i bachi che già sono stati scoperti.

In questi ultimi tempi, grazie anche alle vantaggiose offerte presentate da numerosi Internet provider, si sta diffondendo sempre più il nuovo protocollo di rete IEEE 802.11b. Conosciuto al pubblico come Wireless Internet, o Wi-Fi, permette di connettere con una rete Ethernet senza fili due o più personal computer, con una velocità massima di ben 11 megabit al secondo.

>> Internet senza fili

Alla base di questa tecnologia di rete wireless si utilizzano delle schede di rete, tipicamente connesse a una porta Usb o PcCard (Pcmcia), in quest'ultimo caso installabile nei computer desktop mediante un opportuno convertitore Pci. Grazie a queste schede è possibile superare eventuali ostacoli architettonici senza dover bucare muri per tirare i cavi, anche se ovviamente l'utilizzo prevalente viene fatto nei computer portatili. In molti dei nuovi laptop di fascia alta, inoltre, è già presente il supporto nativo, integrato all'interno del case. I Macintosh hanno invece uno slot di tipo proprietario al quale collegare una scheda Airport (il nome commerciale dato da Apple a questo apparecchio), ma possono comunque utilizzare schede Pc-Card o Pci di altre marche.

Il protocollo, codificato dall'ente internazionale IEEE (www.ieee.org), **prevede due configurazioni di default: Ad Hoc e Infrastructure.** Nel primo caso permette di collegare **due computer direttamente fra loro, in modalità peer-2-peer.** La modalità Infrastructure, quella più complessa, **favorisce la creazione di vere e proprie sottoreti, connesse alla rete fissa attraverso un Access** Point, dispositivo di accesso che si pone concettualmente come una via di mezzo fra un hub e un router. Fra le sue funzioni, oltre a gestire il collegamento fisico fra le antenne, generalmente viene integrata la possibilità di fornire indirizzi Ip in modo dinamico, grazie ad un Dhcp

Alcuni simboli tracciati dai War Driver per segnalare la presenza di reti wireless accessibili.

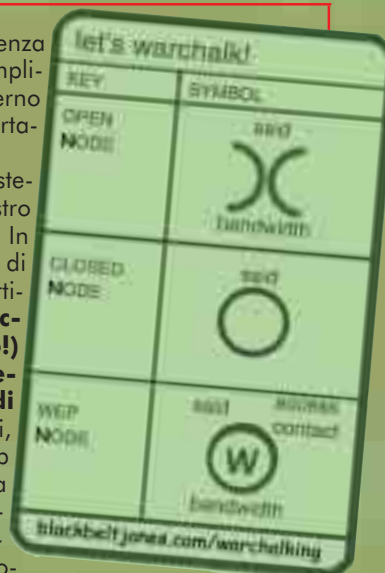
Il gergo dei war-drivers

Come riconoscere se in zona c'è una rete Wireless Ethernet non protetta? Fra i war-drivers si è diffusa una moda, rubata alle abitudini delle logge segrete del 1800: segnare con un gessetto per terra o su un muro un simbolo opportuno, apparentemente privo di senso, ma che un altro war-driver può riconoscere con facilità. I simboli più usati sono due semicerchi verticali, opposti l'uno all'altro, con un nome in alto e un numero in basso indicante la banda disponibile: in questo caso si intende un nodo aperto. In alternativa, troviamo un cerchio con un nome scritto sopra: il nodo in questo caso è chiuso. Se all'interno del cerchio trova posto anche una W, si intende che il nodo trovato è protetto dal protocollo Wep.

server. Sempre l'Access Point gestisce l'eventuale configurazione di sicurezza della rete.

>> Reti sprotette

Se da un lato i vantaggi di un sistema completamente senza fili sono la totale mobilità e l'indipendenza da un luogo fisico, dall'altro c'è il problema che le onde radio non sono "canalizzate" in un flusso privilegiato ma vengono diffuse nell'etere come delle gigantesche bolle elettromagnetiche. Nasce quindi il problema che **chiunque, con una scheda di rete conforme al protocollo o altri dispositivi hardware, può connettersi alla rete, se questa non è opportunamente protetta.** Il protocollo prevede in effetti un sistema per la cifratura dei dati, definito Wep, che però data la sua complessità di gestione non viene sempre attivato dagli amministratori, lasciando quindi le reti di molte aziende aperte alla possibilità di connettersi senza alcun tipo di autenticazione, semplicemente "passeggiando" all'esterno della sede muniti di computer portatile.

È molto diffusa, soprattutto all'estero, ma di recente anche nel nostro paese, la pratica del War-Driving. In che cosa consiste? Ci si arma di portatili, sniffer (vedi il box) e cartina cittadina e **si viaggia in macchina (o anche in elicottero!) attraverso le vie di una metropoli, alla ricerca di punti di accesso radio.** Una volta trovati, si prova a ottenere un indirizzo Ip dal server Dhcp, sempre che la connessione non sia protetta; altrimenti occorre provare a scoprire la chiave di cifratura, operazione che si è dimostrata non impossibile, anzi relativamente semplice, se eseguita con gli appositi tool. I war-drivers usano poi segnare su muri o marciapiedi dei particolari simboli che permettono ad altra gente di collegarsi in rete.

La difesa della rete

Se proprio non si può evitare l'installazione di una rete locale senza fili, ma si desidera renderla il più sicuro possibile, è possibile utilizzare alcuni programmi specificatamente creati.

S-Lan
http://slan.sourceforge.net
S-Lan, o Secure Local Area Network, è un progetto opensource che cerca di garantire una completa affidabilità e sicurezza nelle comunicazioni fra reti wireless e le relative Lan locali, o la rete mondiale Internet. La sua principale differenza rispetto al Wep risiede nella creazione di chiavi temporanee dotate di vita molto breve e costantemente aggiornate. Il software è disponibile per Linux e Windows.

Black Alchemy's Fake AP
http://www.blackalchemy.to/Projects/fakeap/fake-ap.html
Come riportato anche dalla home page, se avere un access point è positivo, averne migliaia può rendere la vita molto difficile ai war-drivers. Con questo programma è possibile generare una cacofonia di segnali, nascondendo così il vero access point da utilizzatori non desiderati.

Le numerose finestre di Wellenreiter, un programma per la ricerca di reti wireless di ogni genere.

>> Reti protette

Vediamo ora come si struttura la protezione contenuta nelle specifiche del protocollo 802.11b. **Il sistema di protezione si chiama Wep, acronimo di Wired Equivalent Privacy,** che dovrebbe rendere impossibili le intercettazioni fra le comunicazioni radio. Utilizza l'algoritmo RC4 in modalità sincrona. Si basa su un sistema a crittazione con due chiavi, una pubblica (chiamata Initialization Vector, di 24 bit) e una privata, inizialmente codificata con una lunghezza di 40 bit, successivamente aumentati a 128 bit quando la legge americana sull'esportazione di tecniche crittografiche lo ha permesso. Utilizzando uno XOR sullo XOR originario dei pacchetti inviati **è possibile risalire all'Initializzation Vector, e decodificare quindi tutte le comunicazioni protette da quella chiave.** La lunghezza di soli 24 bit dell'Initialization Vector permette la creazione di un numero relativamente limitato di codici di crittazione, che fra l'altro non devono nemmeno cambiare ad ogni trasmissione, secondo lo standard: monitorando quindi per un certo tempo una rete wireless è possibile creare una tabella contenente tutte le possibili chiavi di decrittazione, utilizzandole quindi per intercettare i dati e inserirsi nella rete. Esistono alcuni programmi (vedi box) specificatamente creati per forzare il sistema Wep e permettere accessi non autorizzati.

>> Come proteggersi

A questo punto cosa conviene fare? **Se state progettando la costruzione di una rete wireless nella vostra azienda o in casa, tenete conto del fatto che non sarà garantita la sicurezza del 100 %** (ma quando mai, d'altronde?) e che andrà progettata nel migliore dei modi, magari **autenticando gli indirizzi hardware (Mac Address) dei Nic o configurando apposite regole sui firewall. Alternativamente, si può instradare sulla rete wireless un canale VPN (Virtual Private Network) cifrato**, ottenendo un livello di sicurezza sicuramente paragonabile a quello di una rete cablata, anche se purtroppo in questo modo si perderà qualcosa in termini di efficienza e prestazioni.

Francesco Facconi

Wi-Fi Cracker

Una piccola carrellata di programmi che potrebbero essere utilizzati per effettuare l'accesso a reti wireless sprotette, oppure anche protette dal sistema di sicurezza Wep.

802.11B NETWORK DISCOVERY TOOLS
http://sourceforge.net/projects/wavelan-tools/
Si tratta di un programma gafico per Linux che cerca reti Wi-Fi utilizzando l'hardware del portatile. Include la possibilità di memorizzare le coordinate utilizzando un sistema Gps compatibile Nmea collegato alla porta seriale.

WEPCRACK
http://wepcrack.sourceforge.net
Programma opensource testuale studiato per scoprire, utilizzando il metodo descritto da Fluhrer, Mantin e Shamir, la chiave di cifratura del sistema Wep.

AIRSNORT
http://airsnort.shmoo.com
AirSnort è un altro software per Linux utile per il recupero della chiave di cifratura delle Wireless Lan. Monitorizza passivamente le trasmissioni, cercando di decodificare la password, non appena riceve un numero sufficiente di pacchetti.

BSD-AIRTOOLS
www.dachb0den.com/projects/bsd-airtools.html
Software per i sistemi operativi basati su Bsd, consistente in un completo set di programmi per monitorare la rete radio 802.11b. Permette sia di crackare il protocollo Wep, sia di cercare Access Point pubblici.

WALLENREITER
www.remote-exploit.org
Wellenreiter è un programma grafico per la ricerca di reti wireless, segnalando access point e sistemi ad-hoc. Supporta la gestione per le schede costruite da Prism2, Lucent e Cisco. Utilizzando un sistema Gps permette di memorizzare le coordinate geografiche di accesso alla rete. Fra le sue particolarità, la possibilità di girare anche su sistemi Linux/BSD a bassa definizione grafica, come ad esempio un Pda della serie Ipaq.

KISMET
www.kismetwireless.net
Kismet è uno sniffer di reti 802.11b. Permette di cercare tutte le più diffuse tipologie di schede di rete e i relativi protocolli. Una sua funzione crea un disegno dei network riconosciuti, calcolandone la possibile dimensione e adattandoli a delle mappe precedentemente inserite.

UN TROJAN ORMAI SUPERATO MA ANCORA IN CIRCOLAZIONE

IDENTIFICATION
ORDER NO. 10
October 10th 2002

WANTED

DIVISION OF INVESTIGATION
H.J. DEPARTMENT OF NET

CERNUSCO S.N., MI

NAME: NetBus
TYPE: Trojan
ALIAS: NetBus 153, NetBus 160, NetBus 170
DATE OF BIRTH: Marzo 1998
AUTOR: Carl-Fredrik Neikter

Fingerprint Classification

16 O 5 U 001 20
1 17 U 001

Azioni compiute:

A seconda delle versioni, NetBus può effettuare tante azioni diverse. Tra queste le più comuni sono:

Server admin: modifica le impostazioni del server (rimuovere il server, chiuderlo o impostare gli indirizzi IP che possono entrare nel pc).

Start program: esegue un'applicazione.

Screendump: cattura lo schermo.

Get info: mostra informazioni sul PC.

Port redirect: cattura tutti i dati inviati a una porta e li dirotta su un certo indirizzo ip/porta.

App redirect: direziona un qualsiasi programma ad una certa porta del pc.

Listen: esegue un keylog di tutti i dati che la vittima inserisce su tastiera

Control mouse: per controllare il mouse della vittima

Go to url: apre una finestra con un determinato sito internet.

Key manager: legge le password dal disco e dalla memoria.

File manager: permette di scaricare, uploadare e cancellare file.

Mezzi di contagio:

Essere infettati da NetBus significa aver scaricato ed eseguito in qualche modo il Server del Trojan sul proprio PC. Il Server dovrebbe essere riconosciuto dagli antivirus ma il lamer di turno potrebbe usare vari trucchi: il file ha l'estensione exe tipica degli eseguibili ma potreste trovarlo anche come scr (Infatti gli screen saver sono dei veri e propri eseguibili). Inoltre, potrebbe usare un programma tipo WwPack32 per associare l'eseguibile con altri file (immagini, testi ecc.) in modo che vengano eseguiti quando la vittima apre la fotografia o il testo.

Segni particolari:

I Server sono frequentemente dei file con estensione 'exe' che vanno a installarsi in una directory già molto piena (tipo Windows o Windows\System) con nomi simili a file del sistema e icone poco evidenti. Si impostano per partire a ogni avvio del PC modificando il file System.ini, la Cartella di Esecuzione Automatica e soprattutto alcune chiavi del Registro di Configurazione. Una volta avviato, il Server mette in ascolto una certa porta in attesa di ricevere ordini dal Client. A volte l'accesso al Server è protetto da password. Contrariamente a Back Orifice, NetBus non crea processi visibili dall'esterno, per cui risulta difficile da intercettare. A differenza delle prime versioni, il server della versione 2.0 si chiama NBSvr.exe, usa la porta di default 20034 e crea la sua chiamata (nel Registro di Configurazione) al percorso HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

Istruzioni per l'arresto:

Per verificare se il proprio PC è infetto da NetBus si possono usare vari metodi:

- Il server di NetBus adopera per l'autopartenza, all'avvio del PC, una chiamata che si crea nel Registro di Configurazione di Windows. Verificate, mediante Regedit, se vengono eseguiti automaticamente stringhe, file o programmi "sconosciuti". (scelta più consigliata anche se più rischiosa) in: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrenteVersion\Run) vengano richiamate applicazioni sconosciute. In questo caso cancellare la/e stringa e riavviare il computer ed infine cancellare il file del server che trovate nella directory indicata nella stringa del registro che avete eliminato.

N.B. Prima di fare modifiche decisive con SysEdir e Regedit fate una copia di backup dei file da modificare; a un occhio inesperto le stringhe necessarie per l'avvio e il corretto funzionamento del proprio computer possono essere confuse con il nostro "sospettato"!

- Per identificare una generica infezione da trojan esiste un metodo universale: avviare dal buon vecchio DOS il programma 'Netstat' che segnala tutte le porte del vostro sistema attive o in ascolto.
- Si può, in alternativa, adoperare un software come il noto "The Cleaner 3" o "Trojan First Aid Kit 4" (www.sofotex.com/download/software/1743.html).

Ulteriori informazioni:

www.hackfix.org/netbusfix/
www.nwinternet.com/pchelp/nb/netbus.htm

{RoSwEIL}